



日 本 国 特 許 庁
JAPAN PATENT OFFICE

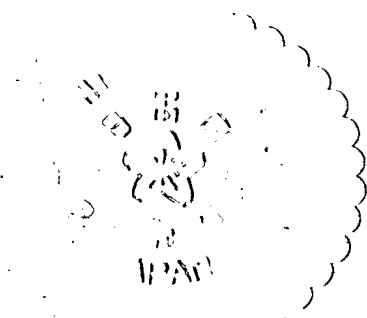
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 6 月 1 8 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 1 7 3 9 8 5
Application Number:
[ST. 10/C] : [J P 2 0 0 3 - 1 7 3 9 8 5]

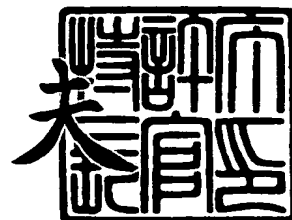
出 願 人 株 式 会 社 東 芝
Applicant(s):



2 0 0 3 年 7 月 1 8 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 14313401

【提出日】 平成15年 6月18日

【あて先】 特許庁長官殿

【国際特許分類】 H04N 1/00

【発明の名称】 送信装置、受信装置、送信制御プログラム及び受信制御プログラム

【請求項の数】 21

【発明者】

【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝
研究開発センター内

【氏名】 斉 藤 健

【発明者】

【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝
研究開発センター内

【氏名】 磯 崎 宏

【発明者】

【住所又は居所】 東京都府中市東芝町 1 番地 株式会社東芝 府中事業所
内

【氏名】 加 藤 拓

【発明者】

【住所又は居所】 東京都青梅市末広町 2 丁目 9 番地 株式会社東芝 青梅
事業所内

【氏名】 小久保 隆

【特許出願人】

【識別番号】 000003078

【住所又は居所】 東京都港区芝浦一丁目 1 番 1 号

【氏名又は名称】 株式会社 東 芝



【代理人】

【識別番号】 100075812

【弁理士】

【氏名又は名称】 吉 武 賢 次

【選任した代理人】

【識別番号】 100088889

【弁理士】

【氏名又は名称】 橘 谷 英 俊

【選任した代理人】

【識別番号】 100082991

【弁理士】

【氏名又は名称】 佐 藤 泰 和

【選任した代理人】

【識別番号】 100096921

【弁理士】

【氏名又は名称】 吉 元 弘

【選任した代理人】

【識別番号】 100103263

【弁理士】

【氏名又は名称】 川 崎 康

【先の出願に基づく優先権主張】

【出願番号】 特願2003- 58927

【出願日】 平成15年 3月 5日

【手数料の表示】

【予納台帳番号】 087654

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1



【物件名】 要約書 1

【包括委任状番号】 0102514

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 送信装置、受信装置、送信制御プログラム及び受信制御プログラム

【特許請求の範囲】

【請求項 1】

暗号化された電子データと、著作権保護用制御データと、前記暗号化された電子データに関する情報を示すペイロードタイプの値を含む RTP (Real-time Transport Protocol) ヘッダと、を有するパケットの送信を制御する送信制御手段と

受信装置との間で、前記ペイロードタイプの値を決めるネゴシエーションを行うネゴシエーション手段と、

前記受信装置との間で、著作権保護のための認証・鍵交換処理を行う認証・鍵交換処理手段と、を備えることを特徴とする送信装置。

【請求項 2】

前記認証・鍵交換処理手段は、ネゴシエーションされた前記ペイロードタイプの値を含むパケットが前記受信装置に送信された後に、前記認証・鍵交換処理を行うことを特徴とする請求項 1 に記載の送信装置。

【請求項 3】

前記送信制御手段は、前記認証・鍵交換処理手段による認証・鍵交換に成功した場合に限り、ネゴシエーションされた前記ペイロードタイプの値を含むパケットを前記受信装置に送信することを特徴とする請求項 1 に記載の送信装置。

【請求項 4】

著作権保護を図る必要のある前記パケットを前記受信装置に送信した後、前記パケットが著作権保護を図る必要があることを報知する情報を前記受信装置に送信する著作権保護報知手段を備えることを特徴とする請求項 1～3 のいずれかに記載の送信装置。

【請求項 5】

著作権保護を図る必要のある前記パケットを前記受信装置に送信する前に、前記パケットが著作権保護を図る必要があることを報知する情報と、前記パケット

の暗号フレームサイズとを、前記受信装置に通知する暗号化情報通知手段を備えることを特徴とする請求項 1～4 のいずれかに記載の送信装置。

【請求項 6】

前記受信装置から送信された、著作権保護を図る必要のある前記パケットの暗号フレームサイズを受信する暗号フレームサイズ受信手段と、

前記パケットを、前記暗号フレームサイズ受信手段で受信された暗号フレームサイズにて暗号化する暗号化手段と、を備えることを特徴とする請求項 1～5 のいずれかに記載の送信装置。

【請求項 7】

前記暗号フレームサイズ受信手段により受信された暗号フレームサイズで前記パケットを送信できるか否かを示す暗号フレームサイズ応答を前記受信装置に送信する暗号フレームサイズ応答送信手段を備えることを特徴とする請求項 6 に記載の送信装置。

【請求項 8】

前記ペイロードタイプの値は、2 種類以上の値、あるいは所定の範囲内の任意の値であることを特徴とする請求項 1～7 のいずれかに記載の送信装置。

【請求項 9】

暗号化された電子データと、著作権保護用制御データと、前記暗号化された電子データに関する情報を示すペイロードタイプと、を含む RTP (Real-time Transport Protocol) を付加したパケットの受信を制御する受信制御手段と、

送信装置との間で、前記ペイロードタイプの値を決めるネゴシエーションを行うネゴシエーション手段と、

前記送信装置との間で、著作権保護のための認証・鍵交換処理を行う認証・鍵交換処理手段と、を備えることを特徴とする受信装置。

【請求項 10】

前記認証・鍵交換処理手段は、ネゴシエーションされた前記ペイロードタイプの値を含むパケットが前記受信装置に送信された後に、前記認証・鍵交換処理を行うことを特徴とする請求項 9 に記載の受信装置。

【請求項 11】

前記受信制御手段は、前記認証・鍵交換処理手段による認証・鍵交換に成功した場合に限り、ネゴシエーションされた前記ペイロードタイプの値を含むパケットを受信することを特徴とする請求項 9 に記載の受信装置。

【請求項 12】

前記著作権保護制御データは、電子データを暗号化するための暗号鍵を生成するのに用いられるシード値の少なくとも一部のビットを含んでおり、

前記シード値を用いて、受信された前記パケットに含まれる暗号化された電子データを復号する復号手段をさらに備えることを特徴とする請求項 9～11 のいずれかに記載の受信装置。

【請求項 13】

前記送信装置が送信した電子データに含まれる前記シード値に基づいて、前記送信装置がシード値を更新したか否かを判断する更新判断手段と、

前記送信装置がシード値を更新したと判断される場合に、前記送信装置に対して認証・鍵交換要求を送信する認証・鍵交換要求手段と、を備えることを特徴とする請求項 12 に記載の受信装置。

【請求項 14】

著作権保護を図る必要のある前記パケットを受信した後、前記パケットが著作権保護を図る必要があることを報知する情報を受信する著作権保護情報受信手段を備えることを特徴とする請求項 9～13 のいずれかに記載の受信装置。

【請求項 15】

著作権保護を図る必要のある前記パケットを受信する前に、前記パケットが著作権保護を図る必要があることを報知する情報と前記パケットの暗号フレームサイズとを受信する暗号化情報受信手段を備えることを特徴とする請求項 9～14 のいずれかに記載の受信装置。

【請求項 16】

著作権保護を図る必要のある前記パケットの暗号フレームサイズを送信する暗号フレームサイズ送信手段を備えることを特徴とする請求項 9～15 のいずれかに記載の受信装置。

【請求項 17】

前記暗号フレームサイズ送信手段が送信した暗号フレームサイズで前記送信装置が電子データを暗号化できるか否かを示す暗号フレームサイズ応答を受信する暗号フレームサイズ応答受信手段を備えることを特徴とする請求項16に記載の受信装置。

【請求項18】

暗号化された電子データと、著作権保護用制御データと、前記暗号化された電子データに関する情報を示すペイロードタイプの値を含むRTP (Real-time Transport Protocol) ヘッダと、を有するパケットの送信を制御するステップと、

受信装置との間で、前記ペイロードタイプの値を決めるネゴシエーションを行うステップと、

前記受信装置との間で、著作権保護のための認証・鍵交換処理とを行うステップと、を備えることを特徴とする送信制御プログラム。

【請求項19】

暗号化された電子データと、著作権保護用制御データと、前記暗号化された電子データに関する情報を示すペイロードタイプと、を含むRTP (Real-time Transport Protocol) を付加したパケットの受信を制御するステップと、

送信装置との間で、前記ペイロードタイプの値を決めるネゴシエーションを行うステップと、

前記送信装置との間で、著作権保護のための認証・鍵交換処理とを行うステップと、を備えることを特徴とする受信制御プログラム。

【請求項20】

著作権保護を図る必要のある前記パケットを前記受信装置に送信する前に、前記パケットをマルチキャストにて送信するか否かを判別するマルチキャスト送信識別手段と、

前記パケットをマルチキャストのパケットにて送信する場合には、前記パケットをマルチキャストの暗号フレームサイズにて暗号化して送信するマルチキャスト暗号化手段と、を備えることを特徴とする請求項1～8のいずれかに記載の送信装置。

【請求項21】

著作権保護を図る必要のある前記パケットを受信した場合、マルチキャストのパケットであるか否かを判別するマルチキャスト受信識別手段と、

前記パケットがマルチキャストのパケットであると判別された場合には、前記パケットをマルチキャストの暗号フレームサイズにて復号化するマルチキャスト復号化手段と、を備えることを特徴とする請求項 9～17 のいずれかに記載の受信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、著作権保護を図る必要の電子データを送信または受信する送信装置、受信装置、送信制御プログラム及び受信制御プログラムに関する。

【0002】

【従来の技術】

デジタル情報家電と呼ばれる商品が増加している。これら商品は、デジタル放送の開始などに伴い、普及が期待される商品群であり、デジタル放送対応テレビや、セットトップボックス、デジタルVTR、DVDプレイヤー、ハードディスクレコーダ等のデジタルデータ・デジタルコンテンツを扱う商品が広く含まれる。

【0003】

この際、考慮すべきは著作権保護である。デジタルデータは、コピー時の品質劣化が無いなどの利点がある反面、容易に不正コピーを行えるなどの欠点も持つ。このため、デジタルAV機器同士をつなぐデジタルネットワークであるIEEE1394には、認証・鍵交換機構や、データの暗号化の機能が兼ね備えられている（非特許文献1参照）。

【0004】

さて、近年、IEEE1394に加えて、家庭内でパーソナルコンピュータ（以下、PC）を用いたネットワーク（イーサネットや無線LAN等）を手軽に構築できるようになった。これは、PCの普及、ブロードバンド環境の低価格化、ネットワーク対応の機器やソフトウェアの普及など、複数の理由が考えられよう。この流れに、AV機器も加わる可能性がある。

【0005】

このような環境で利用されるプロトコルは、主にIP（インターネットプロトコル）である。

【0006】

【非特許文献1】

<http://www.dtcp.com>

【0007】

【発明が解決しようとする課題】

しかしながら、インターネットプロトコル自体は著作権保護を特に考慮に入れていないため、AVデータの著作権保護が十分に図れないおそれがある。特に、最近のように、無線LANやBluetooth等の無線ネットワークが普及している状況では、著作権保護の必要なAVデータが無断で複製や再生される可能性が高くなる。

【0008】

本発明は、このような点に鑑みてなされたものであり、その目的は、著作権保護を図りつつAVデータの送信または受信を行える送信装置、受信装置、送信制御プログラム及び受信制御プログラムを提供することにある。

【0009】

【課題を解決するための手段】

上述した課題を解決するために、本発明は、暗号化された電子データと、著作権保護用制御データと、前記暗号化された電子データに関する情報を示すペイロードタイプの値を含むRTP（Real-time Transport Protocol）ヘッダと、を有するパケットの送信を制御する送信制御手段と、受信装置との間で、前記ペイロードタイプの値を決めるネゴシエーションを行うネゴシエーション手段と、前記受信装置との間で、著作権保護のための認証・鍵交換処理とを行う認証・鍵交換処理手段と、を備える。

【0010】

また、本発明は、暗号化された電子データと、著作権保護用制御データと、前記暗号化された電子データに関する情報を示すペイロードタイプと、を含むRTP（Real-time Transport Protocol）を付加したパケットの受信を制御する受信制

御手段と、送信装置との間で、前記ペイロードタイプの値を決めるネゴシエーションを行うネゴシエーション手段と、前記送信装置との間で、著作権保護のための認証・鍵交換処理とを行う認証・鍵交換処理手段と、を備える。

【0011】

【発明の実施の形態】

以下、本発明に係る送信装置、受信装置、送信制御プログラム及び受信制御プログラムについて、図面を参照しながら具体的に説明する。

【0012】

以下では主に、音声や映像のAVデータを送受する例を説明するが、本発明は、AVデータ以外の各種電子データに適用可能である。

【0013】

（第1の実施形態）

図1は本発明の一実施形態である送信装置と受信装置とを備えたAV通信システムの概略構成を示すブロック図である。図1のAV通信システムは、ある家庭内のホームネットワーク1と、このホームネットワーク1に接続されている送信装置2及び受信装置3とを備えている。ホームネットワーク1の一例として、以下では無線ネットワーク1について説明するが、無線ネットワーク1の代わりに、あるいは無線ネットワーク1と並行して、イーサネットやIEEE1394等の有線ネットワークを用いてもよい。無線ネットワーク1の具体的な形態は特に問わないが、例えば、IEEE802.11a、IEEE802.11bまたはIEEE802.11gなどの各種の無線LANが考えられる。

【0014】

送信装置2と受信装置3は、AVデータのやり取りを行う。送信装置2は、セットトップボックスやDVDプレイヤー等のAVデータの送信装置となりうる機器である。受信装置3は、テレビ、表示装置、スピーカ、AV録画・録音装置などのAVデータの受信装置となりうる機器である。

【0015】

図2は送信装置2の内部構成の一例を示すブロック図である。図2の送信装置2は、インタフェース部11と、AVデータ生成／蓄積部12と、RTP (Real-time

Transport Protocol) 処理部 13 と、著作権保護暗号化部 14 と、パケット処理部 15 と、通信処理部 16 と、著作権保護認証・鍵交換部 17 と、AV制御部 18 とを有する。

【0016】

インタフェース部 11 は、無線ネットワーク 1 に接続される部分であり、無線ネットワーク 1 に対して AV データ等を送信する。AV データ生成／蓄積部 12 は、受信装置 3 に送信するための AV データの生成や蓄積を行う。RTP 処理部 13 は、タイムスタンプ処理やシーケンス番号処理などのトランスポート層層の処理と、再生や停止などの AV 制御とを行う。通信処理部 16 は、AV データを含むデータリンク層のフレーム（以下では、データリンク層のフレームの例としてイーサネットフレームを用いることとする）を生成して送信するとともに、無線ネットワーク 1 を介して受信したイーサネットフレームを受信する。著作権保護認証・鍵交換部 17 は、著作権保護のために、受信装置 3 との間で認証や鍵交換処理を行う。

【0017】

図 3 は受信装置 3 の内部構成の一例を示すブロック図である。図 3 の受信装置 3 は、インタフェース部 21 と、通信処理部 22 と、パケット処理部 23 と、著作権保護復号化部 24 と、RTP 処理部 25 と、AV データ再生／蓄積部 26 と、著作権保護認証・鍵交換部 27 と、AV 制御部 28 とを有する。

【0018】

通信処理部 22 は、インタフェース部 21 にて受信された受信パケットからデータリンク層のフレーム（この例ではイーサネットフレーム）を抽出する。パケット処理部 23 は、通信処理部 22 で受信されたイーサネットフレームから UDP/IP パケットまたは TCP/IP パケットを抽出する。著作権保護復号化部 24 は、著作権保護のために暗号化されて転送されてきた AV データを復号化する。RTP 処理部 25 及び著作権保護認証・鍵交換部 27 はそれぞれ、RTP 処理部 13 と著作権保護認証・鍵交換部 17 と同様の処理を行う。

【0019】

著作権保護認証・鍵交換部 27 が行う認証・鍵交換処理の少なくとも一部は、

IPパケットを用いてなされてもよいし、IPパケットを用いずに、認証・鍵交換プロトコルを直接イーサネットフレーム上に載せて行ってもよい。図2の送信装置2と図3の受信装置3は、認証・鍵交換プロトコルに利用するデータを直接イーサネットフレーム（または802.11フレーム）上に載せる場合のブロック構成を図示したものである。

【0020】

本実施形態の送信装置2と受信装置3でやり取りされるデータフォーマットは図4のようなものである。データ本体を表すペイロードd1にトランスポート層ヘッダd2を付加したUDP/IPパケットに、データリンクヘッダd3を付加してデータリンクフレームが生成される。すなわち、AVデータはまずUDP/IPパケットにカプセル化され、さらにUDP/IPパケットは、データリンクフレームにカプセル化される。また、データリンクフレームには物理層ヘッダd4が付加される。

【0021】

なお、データリンク層のフレームフォーマットとしては、イーサネットフレームや802.11フレームを用いればよい。802.11フレームの場合、無線ネットワーク1上でのみ使用される制御データ、例えばIEEE802.11無線LANにおけるFCフィールドやDur/IDフィールドなどが含まれるが、図4では簡略化のためにこれらの存在を無視している。

【0022】

また、トランスポート層のプロトコルとしては、UDP (User Datagram Protocol) やTCP (Transmission Control Protocol) を用い、ネットワーク層のプロトコルとしてはIP (Internet Protocol) を用いればよい。ホームネットワーク1が無線ネットワーク1の場合には、イーサネットフレームにさらに無線レイヤヘッダを付加して無線レイヤフレームが生成され、この無線レイヤフレームが送信装置2から送信される。

【0023】

図4では、簡略化のために、トレイラの存在を無視している。無線レイヤヘッダには、無線ネットワーク1上でのみ使用される制御データ、例えばIEEE802.11無線LANにおけるFCフィールドやDur/IDフィールドなどが含まれる。

【0024】

本実施形態では、著作権保護を図る必要のあるAVデータを暗号化して送信する。暗号化するのは、図4のUDP/IPパケットのペイロード部分である。このペイロード部分のより詳細なデータフォーマットは図5のようなものである。AVデータを暗号化したペイロードd5に、IETFにて標準化されたAVデータ転送用の転送プロトコルであるRTP (Real-time Transport Protocol) ヘッダd6と、UDP/IPヘッダd7とを付加し、さらに、RTPヘッダd6とペイロードd5との間に、著作権保護用制御データd8を付加する。この著作権保護用制御データd8は、コピー制御情報（以下、CCI）や、AVデータに対して施される暗号化の鍵の値の変化のタイミングを通知するためのビットなどからなる。著作権保護用制御データd8は、RTPヘッダの中に含めてもよい。また、著作権保護用制御データd8の一部がAVデータと共に暗号化されていてもよい。なお、RTPについては、<http://www.ietf.org/rfc/rfc1889.txt>を参照されたい。

【0025】

RTPヘッダd6には、ペイロードタイプd9が定義されている。本実施形態では、RTPヘッダのペイロードタイプd9の値として、ダイナミック・ペイロードタイプの値（#z）を用いる。ここで、ダイナミック・ペイロードタイプの値を用いるとは、符号化方式ごとに予め定められている割り当て済みのペイロードタイプの値を用いるのではなく、通信ごとに事前にネゴシエーションを行い、利用するペイロードタイプの値を動的に（ダイナミックに）ネゴシエーションした上で決定することを意味する。ネゴシエーションは図2及び図3のAV制御部18、28が行う。

【0026】

これは、従来のRTPと異なり、ペイロードが暗号化されているため、従来のRTPフォーマットとは異なるデータがペイロードに入るという事情と、RTPヘッダとペイロードの間に著作権保護用制御データd8が入るという事情による。すなわち従来のRTPのフォーマットと、著作権保護用制御データd8が挿入された時のフォーマットが異なるため、RTPパケットを受信した受信装置3は、どちらのフォーマットであるか、あるいは受信したパケットが暗号化されており、復号化が

必要なデータなのか否かを識別する必要がある。

【0027】

図6は送信装置2と受信装置3が行うAVデータの暗号化伝送処理の第1の実施形態の処理手順を示すシーケンス図である。以下、この図に基づいて、第1の実施形態の暗号化伝送処理を詳しく説明する。なお、著作権保護の仕組みとして、例えば、DTCP (Digital Transmission Content Protection) を想定する。なお、DTCPの詳細については、<http://www.dtcp.com>を参照されたい。

【0028】

まず、受信装置3は、送信装置2に対してAVデータの送信を要求する(ステップS1)。ここでは、IETFが規定したAVストリーミング機能の遠隔制御用のプロトコルであるRTSP (Real Time Streaming Protocol: RFC2326参照) を用いて、TCP/IP上にてコマンド(プロトコル)のやり取りを行う。なお、RTSP以外に、IEEE1394におけるAV/Cや、UPnP (ユニバーサル・プラグアンドプレイ) プロトコル等によっても、同様の制御を行うことができる。

【0029】

RTSPでは、(1)AVストリーミング伝送に用いられる符号化方式と、そのビットレート等の各種の属性やパラメータ、(2)使用されるトランスポートプロトコル(TP)の種別(本実施形態の場合はRTP/UDP)、(3)RTPで用いられるペイロードタイプの値(本実施形態の場合、ダイナミック・ペイロードタイプの値を用いる)、(4)通信を行うTCP、またはUDPポート番号の値(本実施形態の場合はTCPを用いる。もちろん、実際にはUDPを用いても良い)、(5)ストリーミングの動作の規定(再生、巻き戻し、停止等)等についてのネゴシエーションを行う。

【0030】

上記(1)～(5)等で、送信装置2と受信装置3間で合意が得られると、送信装置2は、AVデータを暗号化した後(ステップS2)、上記RTSPで合意されたコネクション(本実施形態では、送信装置2のIPアドレス=a、送信ポート番号=#x、受信装置3のIPアドレス=b、受信ポート番号=#y)にて、転送プロトコル=RTP、合意されたダイナミック・ペイロードタイプ(PT)の値(=#z)にて、暗号化されたAVデータを含むAVストリームの送信を開始する(ステップS3)

。

【0031】

ステップS3で送信されるAVストリームは図5のようなデータフォーマットである。このAVストリームを受信した受信装置3が、例えばAVストリーム中の著作権保護用制御データd8により、受信したAVデータに暗号がかけられていることを発見したとする。この場合、受信装置3は送信装置2に対して認証・鍵交換手順を要求し（ステップS4）、送信装置2との間で認証・鍵交換処理を行う（ステップS5）。認証・鍵交換処理に成功すると、受信装置3は、復号鍵を入手する（ステップS6）。

【0032】

著作権保護用制御データd8内の構成は、転送されるAVストリームのトランスポート層のプロトコルにより異なってもよい。例えば、トランスポート層のプロトコルがTCPの場合は、暗号化されたAVデータのサイズを示すLengthフィールドを定義してもよい。もちろん、トランスポート層のプロトコルがUDPであっても、Lengthフィールドが定義されていてもかまわない。

【0033】

この認証・鍵交換の要求と認証・鍵交換処理は、TCP/IPパケット上で行ってもよいし、無線レイヤフレームやイーサネットフレーム上に、認証・鍵交換用のデータを直接載せて行ってもよい。また、この認証・鍵交換手順は、ホームネットワーク1内に留まるべきものであるため、TCP/IPパケット上で行う場合には、TTL (Time To Live) の値をホームネットワーク1内でのみ到達可能な値（たとえば「1」）にした状態で通信を行う等の制限を設けるのが望ましい。

【0034】

認証・鍵交換は、特定のRTPストリームで転送されるAVストリームに関して行われる。このため、認証・鍵交換を行う前提として、「どのAVストリームに関する認証・鍵交換なのか」についてのネゴシエーションを行う必要がある場合がある。

【0035】

例えば、受信装置3が、受信したAVストリームが暗号化されていることを認識

し、「このAVストリームについての認証・鍵交換をさせて欲しい」と送信装置2に問い合わせる場合がある。また、送信装置2が、「このAVストリームは、暗号化して受信装置3に対して送出する。このことを、予め、あるいは、AVストリーム転送と同時に、受信装置3に対して通知し、認証・鍵交換のトリガをかけさせる必要がある」と判断し、受信装置3に対して、「このAVストリームは暗号化して送信する。よって、このAVストリームについて認証・鍵交換手順を送信装置2に対して行うべし」という通知を行う場合も考えられる。

【0036】

もちろん、AVストリーム毎に個々に認証・鍵交換を行うのではなく、「送信装置2と受信装置3の間でやり取りされる、全てのRTPストリームに関して有効とするための認証・鍵交換」を最初に行い、その後は、同送信装置2と受信装置3の間でやり取りされる全てのRTPストリームに関して、上述した認証・鍵交換手順で定められた条件に従って、AVデータの暗号化を行ってもよい。

【0037】

あるいは、特定のペイロードタイプの値については著作権保護を施すことを、送信装置2と受信装置3の間で予め合意しておき、このようなペイロードタイプの値をもつRTPストリームが受信された場合には、著作権保護が施されているものとしても良い（もちろん、RTSP内にて、設定しているRTPセッションにDTCP著作権保護が施されていることをネゴシエーションする方法も考えられる）。

【0038】

上述した図6は受信装置3が送信装置2に対して認証・鍵交換のトリガをかける場合の処理手順を示している。受信装置3は、何らかの方法で、受信したAVストリームが暗号化されていることを認識する。例えば、「受信したAVストリームを複号しても、所望のAVストリームを再生できない場合」、あるいは「受信したAVストリームに、図5のような著作権保護用制御データd8が付属しており、これを検出して、そのAVストリームが暗号化されていることを認識する場合」、「RTPのペイロードの値としてダイナミックペイロード用の値が用いられており、この値が、データが暗号化されている場合に使われる値であることを認識している場合」等が考えられる。

【0039】

受信したAVストリームが暗号化されていること、あるいはその可能性があることを認識した受信装置3は、認証・鍵交換要求を送信装置2に対して送出する。この手順もDTCPの手順の一部とすることが可能である。この場合、受信装置3は、その認証・鍵交換要求（あるいは、後続の認証・鍵交換手順パケット）にて、「どのAVストリームについての認証・鍵交換であるか」を明示する。本実施形態では、転送プロトコル種別（RTP）とRTPパケットのペイロードタイプの値（#z）の値を使う。

【0040】

ちなみに、送信装置2のIPアドレスとポート番号、及び受信装置3のIPアドレスとポート番号を、その認証・鍵交換要求に明記してもよいし、RTPのSSRCフィールドの値（AVソース毎に一意につけられる識別番号。詳細は、RTPのスペックであるRFC1889を参照のこと）、あるいはIPv6パケット等に含まれる「フローID」の値を用いても良い。

【0041】

これを受信した送信装置2は、その認証・鍵交換要求（あるいは、認証・鍵交換手続き）が、どのペイロードタイプの値のAVストリームを対象としたものであるかを認識した上で、認証・鍵交換手順を継続する。

【0042】

認証・鍵交換手順が終了すると、受信装置3は、その認証・鍵交換結果をもとに、その暗号化AVストリームの復号鍵を入手（あるいは、入手するための計算のための初期情報を取得）することができる（ステップS6）。

【0043】

なお、本実施形態において、コンテンツを暗号化するために用いる鍵 K_z は、送信装置2と受信装置3の間の認証・鍵交換処理によって生成された鍵 K_a と、認証・鍵交換が成立した後に送信装置2によってセッション毎にランダムに設定される複数ビット（たとえば64ビット）からなる値 K_b （以後、 K_b をシード値とよぶ）を入力とする関数 f によって生成された値を用いることとする。すなわち、 K_z は以下の式によって求められる。

【0044】

$$K_z = f(K_a, K_b)$$

また、ここでは、送信装置2が鍵 K_a を別な値に設定した時には、必ずシード値 K_b を初期化する(ランダムに設定しなおす)こととする。さらに、 K_b はAVデータ送信中に送信装置2が一定周期ごとに値を常に更新することとする。

【0045】

従来は、著作権保護用制御データ d_8 の中に、 K_b の下位1ビットを挿入するフィールドが定義されており、送信装置2はこのフィールドに、コンテンツを暗号化する鍵である K_z を計算する際に用いた K_b の下位1ビットを入れて送信する。

【0046】

図7は著作権保護用制御データ d_8 のデータフォーマットを示す図である。なお、著作権保護用制御データ d_8 には、シード値 K_b の下位 N ビット d_{10} と、暗号データパディング長 d_{11} が含まれていてもよい。

【0047】

AVデータを暗号化する際に用いる暗号アルゴリズムによっては、暗号化のサイズが固定長の倍数単位(例えば8バイトの倍数ごと)に制限される場合がある。例えば、8バイトごとにデータを暗号化するアルゴリズムを用いる場合、14バイトのデータを暗号化するには、元のデータに2バイトのパディングをつける必要がある。この暗号データパディング長 d_{11} は、受信装置の側で何バイトのパディングを挿入したのかを知らせるために用いる。実際の値としては、パディングしたバイトの値でもよいし、パディングする前のデータ長、あるいはそれらの値をコード化した値でもよい。

【0048】

図8は従来の K_a 、 K_b 、 K_z の処理方法を示す図である。まず、送信装置2と受信装置3は認証・鍵交換処理を行う(ステップS81)。認証・鍵交換が成功すると、送信装置2と受信装置3は鍵 K_a を共有することができる(ステップS82, S83)。前述のようにAVデータは、この鍵 K_a とシード値 K_b を入力とする関数 f によって生成された値 K_z によって暗号化される。

【0049】

次に、送信装置2はシード値 K_b を初期化($K_b = A$)する(ステップS84)。受信装置3は送信装置2に対してシード値 K_b の問い合わせを行い(ステップS85)、送信装置2はシード値 A を受信装置3に送信する(ステップS86)。受信装置は、受信されたシード値 A を設定する(ステップS87)。

【0050】

送信装置2は、 $K_z = f(K_a, A)$ にてAVデータを暗号化し(ステップS88)、暗号化したAVデータを送信する(ステップS89)。このとき、AVデータの著作権保護用制御データ d_8 の中に現在のシード値 K_b の下位1ビットをつけて送信する。

【0051】

受信装置3はAVデータの著作権保護用制御データ d_8 の中に含まれるシード値 K_b の下位1ビットの値と、 K_a とを元にAVデータを復号化するための鍵 K_z を計算し、AVデータを復号する(ステップS90)。

【0052】

なお、各AVデータには下位1ビットしか含まれていないため、受信装置3は K_a と K_b の下位1ビットからだけでは K_z を計算することができない。そこで、認証・鍵交換処理の後に、受信装置3は、上記のステップS85にて、送信装置2によって設定された K_b の全ビットの値を問い合わせる処理を行う。

【0053】

これにより、受信装置3は、最初の一回だけ K_b の値を知り、その後はAVデータの著作権保護用制御データ d_8 の中に含まれる K_b の下位1ビットの変化を観察することで、送信装置2が K_b を更新したことを検出することができ、更新後のシード値と K_a からコンテンツを復号化する鍵の値を計算することができる。ここで重要なことは、著作権保護用制御データ d_8 の中に定義されている K_b の1ビットは K_b の値の変化のタイミングを通知することに用いられている点である。

【0054】

上述したように、送信装置2はAVデータ送信中に K_b の値を更新する(ステッ

プS91)。なお、更新の方法には、時間によって更新する方法と、送信するAVデータのバイト数ごとに、一定の間隔で（たとえば1づつ）更新する方法がある。ここでは説明を簡略化するために、一定バイト数ごとにシードの値を1づつ増加させることとする。

【0055】

図8では、送信装置2がKbの値をAからA+1に更新したことを示している。Kbの更新によってコンテンツの暗号化に用いる鍵Kzの再計算を行う。具体的にはKaとA+1から関数fを用いて計算した値Kz'を求める。このKz'を用いてコンテンツを暗号化して送信する（ステップS92, S93）。なお、Kz'によって暗号化されたAVデータの著作権保護用制御データd8の中にはA+1の下位1ビットを含める。

【0056】

このAVデータを受信した受信装置3はAVデータの著作権保護用制御データd8の中に含まれるKbの下位1ビットの値から、KbがAからA+1に変化したことを知ることができ（ステップS94）、KaとA+1から関数fを用いてコンテンツを復号する鍵Kz'の値を計算することができる。これにより、受信したAVデータを正しく復号することができる（ステップS95）。

【0057】

なお、シード値の問い合わせや応答に用いるメッセージは認証・鍵交換で用いるメッセージと同様に、IPパケットを用いてなされてもよいし、IPパケットを用いずに、認証・鍵交換プロトコルに利用するデータを直接802.11フレーム（またはイーサネットフレーム）上に載せて行ってもよい。

【0058】

図9は送信装置2のコンテンツ鍵更新の検出処理手順を示すシーケンス図である。以下、図9を参照しながら、本実施形態の特徴である著作権保護用制御データd8の中に含めるシード値Kbを、下位1ビットではなく下位複数ビットに設定することの効果について説明する。ここでは、シード値Kbが一定周期で更新され、現在の値がBになっているものとする。

【0059】

まず、送信装置 2 は、暗号鍵 $K_{z1} = f(K_a, B)$ で AV データを暗号化して（ステップ S 101）、受信装置 3 に送信する（ステップ S 102）。受信装置 3 は、この AV データを復号鍵 $K_{z1} = f(K_a, B)$ で復号する（ステップ S 103）。

【0060】

ここで、送信装置 2 が AV データの出力を停止したり、再起動したりする等の理由により、受信装置 3 と共有していた K_a を破棄し（ステップ S 104）、新しい値 K_a' に更新したとする（ステップ S 105）。これと同時にシード値も初期化され、 B とは異なる値 C に再設定される（ステップ S 106）。

【0061】

RTP においては、下位レイヤにコネクションレス型のプロトコル UDP を用いることが一般的である。コネクションレス型のプロトコルでは、受信装置と送信装置は互いに状態を保持しないため、仮に送信装置 2 がセッションを破棄したとしても、受信装置 3 はこれを検出することができない。

【0062】

従って、従来方法においては仮に送信装置 2 が再起動して鍵の値を K_a' に更新したとしても、そのことを受信装置 3 が知る手段がない。またコネクションレス型のプロトコルを使った場合、送信装置と受信装置の間の伝送系路上でパケットが喪失した場合や、受信装置がパケットを受信できなかった場合には、このパケットロスが行ったことを知る手段がない。しかし、著作権保護用制御データ d_8 の中に含めるシード値 K_b を、下位複数ビットに設定することで、 K_a の変化を受信装置 3 で検出したり、パケットロスが起こったりしたことを検出することができる。その理由を以下に示す。

【0063】

まず、シード値の変化を検出する手段について述べる。受信装置 3 と共有していた K_a を送信装置 2 が破棄し、新しい値 K_a' に更新したとする。送信装置 2 は、再設定された鍵 K_a' とシード値 C を用いてコンテンツを暗号化する鍵 K_{z2} を求め、 K_{z2} によって AV データを暗号化して送信する（ステップ S 107, S 108）。この AV データを受信した受信装置 3 は、著作権保護用制御データ d

8の中に含めるシード値の下位NビットがCであり、これまで受信してきた値BまたはBを更新した値B+1ではないことが分かる。

【0064】

Kbのビット長が十分に長ければ、初期化によってランダムに設定された値(C)と、以前に利用していた値(BないしB+1)が一致する確率は低く、受信装置は期待していた値BまたはB+1ではないAVデータを受信した場合、送信装置2は鍵Kaを更新したことを暗号処理の中で検出することができる(ステップS109)。

【0065】

次に、送信装置と受信装置の間の通信経路上でパケットロスが発生したことを検出する方法について述べる。

【0066】

図10にAVデータの中の著作権保護用制御データd8の中に含めるシード値を下位1ビットにした場合の処理手順の一例を示す。送信装置2と受信装置3がシード値を共有するまでは図8のステップS86と同様の手順でよい。ここで仮に共有したシード値をEとする(ステップS121)。また、Eの最下位ビットは0であるとする。送信装置2は前述したルールにより、一定周期ごとにシード値を更新する(ステップS128)。ここでは、EからE+1、E+2、E+3と更新することとする。すなわち、E+1の最下位ビットは1であり、E+2の最下位ビットは0、E+3は1である。

【0067】

AVデータに付属する著作権保護用制御データd8の中に含めるシード値が下位1ビットである場合、送信装置2がシード値Eで暗号化したAVデータについては、受信装置3は、Eの最下位ビットである0を受信し、送信装置2のシード値がE+1、E+2、E+3と更新される度に1、0、1の順で受信し、E+1、E+2、E+3のシード値で受信したAVデータを復号化する(ステップS124, S127, S132)。

【0068】

次に、パケットロスが発生した場合の処理手順を図11に示す。シード値Eに

てAVデータが送受信されるまでは図12と同様の手順でよい。ここで仮に受信装置3はシード値を $E+1$ としたデータすべての受信に失敗したとする（ステップS145, S146）。

【0069】

コネクションレスのプロトコルでは、損失したデータの再送は行わないため、受信装置3は $E+1$ のデータの受信に失敗したことを知ることはできない。すなわち、受信装置3は、シード値が E の最下位ビット0を受信した後、シード値 $E+2$ の最下位ビット0を受信するため、シード値の更新は行われず、送信装置2はシード値 $E+2$ にてAVデータを暗号化しているにもかかわらず、受信装置3はシード値 E にて受信したAVデータを復号化するため、正しく復号化することができない（ステップS150）。

【0070】

一方、著作権保護用制御データd8の中に含めるシード値を下位複数ビットである場合の処理手順を図12に示す。この図では説明を簡略化するために、シード値のビット数を3ビットとしてある。この場合、受信装置3は仮にシード値 $E+1$ で暗号化されたデータの受信に失敗したとしても、 $E+2$ で暗号化されたデータに含まれるシード値の値を確認することで（ステップS169）、シード値が更新されたことを検出することができ、AVデータを正しく復号することができる（ステップS170）。

【0071】

同様の目的を達成するには、シード値のすべてのビットを著作権保護用制御データd8に含めたり、コンテンツ暗号鍵の番号を新たに定義したりすることでも可能である。しかし、すべてのビットを転送する場合と比較して、シード値の下位 N ビットを転送することで、ヘッダの大きさを抑えることができ、AVデータを効率よく転送することができる。

【0072】

図13は、著作権保護用制御データd8の中に含めるシード値 Kb を、下位複数ビットに設定する場合の受信装置3の内部構成を示すブロック図である。図3との違いは、受信したAVデータの著作権保護用制御データd8の中に含まれるシ

ード値の値が、以前受信したシード値と同じか、あるいはそのシード値から予測可能な値（たとえば1大きい値）であるか否かを判定し、もし期待された値でなかった場合には認証・鍵交換をやり直すことを著作権保護認証・鍵交換処理部に通知する機能をもつシード値更新検出部29を持つ点である。

【0073】

このように、第1の実施形態では、著作権保護の必要なAVデータを暗号化したペイロードに、プロトコル種別（例えばRTP）と、このプロトコルが使用するペイロードタイプの値と、を付加したAVストリームを送信装置2から受信装置3に送信するため、このAVストリームを受信した受信装置3は、AVデータが暗号化されていることを容易に検出でき、かつ認証・鍵交換が必要なデータを容易に識別できる。これにより、著作権保護を図りつつ、AVデータを簡易かつ迅速に受信及び再生できる。

【0074】

また、復号鍵を生成するためのシード値をそのまま受信装置3に送信するのではなく、シード値の一部のビットのみを受信装置3に送信することにより、AVデータのデータ量を抑制できるとともに、セキュリティ性も向上できる。

【0075】

（第2の実施形態）

第2の実施形態は、AVデータを暗号化して送信したことを送信装置2から受信装置3に通知するものである。

【0076】

第2の実施形態の送信装置2及び受信装置3はそれぞれ図2及び図3と同様に構成されているが、AVデータの暗号化伝送処理の一部が第1の実施形態と異なっている。

【0077】

図14は送信装置2と受信装置3が行うAVデータの暗号化伝送処理の第2の実施形態の処理手順を示すシーケンス図である。第2の実施形態では、送信装置2が受信装置3に暗号化されたAVデータを含むAVストリームを送信した後に（ステップS13）、AVデータが暗号化されていることを通知するためのAVストリーム

暗号化通知を送信装置 2 が受信装置 3 に送信する (ステップ S 1 4)。この通知は、送信装置 2 が送信した AV ストリーム (ペイロードタイプ = # z) が DTCP 等のプロトコルに従って暗号化され、これを受信装置 3 が復号するには、送信装置 2 との間で認証・鍵交換を行う必要があることを受信装置 3 に知らせるものである。この通知は、IP パケットを用いて行ってもよいし、無線レイヤパケット、もしくはイーサネットフレームを用いて行ってもよい。またはコンテンツ指定の応答メッセージとして、「コンテンツを暗号化して送信する」ことを HTTP のレスポンスメッセージの中にも含めてもよいし、SDP (Session Description Protocol: RFC 2327 参照) を拡張した形式で送信してもよい。

【0078】

図 15 は、受信装置 3 が送信装置 2 に対して所望の AV データを指定し、その指定に対する応答として、当該 AV データが暗号化されていることを通知する場合の処理手順を示すシーケンス図である。

【0079】

まず、受信装置 3 は、AV 制御コマンドを送信装置 2 に対して送信した後 (ステップ S 2 1)、AV データのコンテンツを指定する (ステップ S 2 2)。このコンテンツの指定方法としては、例えば HTTP 等の公知の手法を用いればよい。

【0080】

送信装置 2 は、指定されたコンテンツが著作権を保護すべきコンテンツであることをコンテンツの付加情報等から認識し (ステップ S 2 3)、AV データを暗号化して送信した後 (ステップ S 2 4, S 2 5)、AV ストリーム暗号化通知を HTTP のレスポンスメッセージまたは SDP にて送信する (ステップ S 2 6)。これにより、受信装置は、送信装置 2 との間で認証・鍵交換を行う必要があることを知る。

【0081】

受信した AV ストリーム (ペイロードタイプ # z の AV ストリーム) が暗号化されることを認識した受信装置 3 は、認証・鍵交換要求を送信装置 2 に対して送信し (ステップ S 2 7)、送信装置 2 と受信装置 3 との間で認証・鍵交換処理を行う (ステップ S 2 8)。

【0082】

なお、図14及び図15では、ペイロードタイプの値として特定の値(#z)を通知する形の例を示したが、著作権保護を施すペイロードタイプの2種類以上の値からなる範囲(例えば#z1～#z2の範囲の値)を通知してもよい。

【0083】

このように、第2の実施形態では、AVストリーム中のAVデータが暗号化されていることを送信装置2が受信装置3に通知するため、受信装置3は、受信したAVストリーム中のAVデータが暗号化されているか否かを自分自身で調べる必要がなくなる。したがって、受信装置3の処理を軽減できるとともに、認証・鍵交換処理が完了するまでの時間を短縮できる。

【0084】

(第3の実施形態)

第3の実施形態は、AVデータを送信する前に、著作権保護のための認証・鍵交換を行うものである。

【0085】

第3の実施形態の送信装置2及び受信装置3はそれぞれ図2及び図3と同様に構成されているが、AVデータの暗号化伝送処理の一部が第1及び第2の実施形態と異なっている。

【0086】

図16は送信装置2と受信装置3が行うAVデータの暗号化伝送処理の第3の実施形態の処理手順を示すシーケンス図である。まず、受信装置3は、送信装置2に対して、IPパケットまたはイーサネットフレームにて、認証・鍵交換を要求する(ステップS31)。そして、送信装置2と受信装置3との間で、認証・鍵交換処理を行い(ステップS32)、認証・鍵交換処理に成功すると、受信装置3は復号鍵を取得する(ステップS33)。

【0087】

この認証・鍵交換の間に、「RTPのペイロードタイプの値が#z1～#z2の場合には、そのRTPセッションのデータはDTCPにて著作権保護のための暗号化が施されており、更にRTPヘッダとRTPペイロードの間にDTCP用の制御データが

挿入される」ということを、認証・鍵交換の段階で送信装置2と受信装置3の間で共有する。

【0088】

その後、受信装置3は、送信装置2に対してAVデータの送信を要求し（ステップS34）、これを受けて送信装置2はAVデータを暗号化し（ステップS35）、図4のフォーマットのIPパケットまたはイーサネットフレームを受信装置3に向けて送信する（ステップS36）。図16の例では、ペイロードタイプの値の範囲を#z1～#z2にして、暗号化したAVデータを伝送している。

【0089】

受信装置3は、ペイロードタイプの値を参照することで、そのAVストリームがDTCPにて暗号化されていることを認識でき、適切な復号化手順を経て、AVストリームの再生を行うことができる。

【0090】

この他にも、認証・鍵交換手順に、対象とするペイロードタイプの値を含めておき、そのコマンドが要求する何らかの手順（例えば、最新の鍵の値を問い合わせる等）の対象が、特定のペイロードタイプのAVストリームについてのものであることを通知する手順を加えてもよい。

【0091】

このように、第3の実施形態では、受信装置3から認証・鍵交換要求を行って、認証・鍵交換処理に成功した場合に限り、送信装置2から受信装置3に対して、暗号化したAVデータを含むAVストリームを送信するため、無駄にAVストリームを送信しなくて済み、通信効率の向上が図れるとともに、セキュリティ性も向上する。

【0092】

（第4の実施形態）

第4の実施形態では、送信装置2がAVデータを送信するに先立ち、受信装置3とAVデータの暗号フレームサイズの決定を行うものである。

【0093】

第4の実施形態における送信装置2はAVデータをある一定のサイズに分割し、

暗号化して受信装置 3 に送信する。なお、分割されたこの 1 つの暗号フレームは、単一の暗号ブロックで構成されていてもよいし、暗号ブロックをチェーンさせた暗号ブロックチェーン（CBC：Cipher Block Chain）であってもよい。暗号フレームサイズとは、単一の暗号ブロックの場合はブロック長を指し、暗号ブロックチェーンの場合はチェーンさせた時のサイズを指す。

【0094】

送信装置 2 と受信装置 3 が AV データの暗号フレームサイズを合意する方法には、(1)送信装置 2 と受信装置 3 があらかじめ合意したサイズとする方法、(2)送信装置 2 から受信装置 3 へ通知する方法、(3)受信装置 3 から送信装置 2 へサイズを通知する方法、(4)(1)から(3)の方法を組み合わせた方法、など種々の方法がある。

【0095】

(1)の場合、各ベンダーは予め文書等で定められた暗号フレームサイズに従って送信装置 2 はデータを暗号化し、受信装置は復号化する方法である。

【0096】

(2)は、送信装置が AV データ送信に先立ち、受信装置へ暗号フレームサイズを指定する方法である。

【0097】

図 17 は送信装置 2 と受信装置 3 が行う AV データの暗号化伝送処理の第 3 の実施形態の処理手順を示すシーケンス図である。まず、受信装置 3 は、送信装置 2 に対して AV データの送信を要求する（ステップ S 4 1）。これを受けて、送信装置 2 は AV データの暗号化を行う（ステップ S 4 2）。

【0098】

次に、送信装置 2 は、AV データが暗号化されていることを通知するための AV ストリーム暗号化通知を受信装置 3 に送信する（ステップ S 4 3）。ここまでは第 2 の実施形態と同様である。

【0099】

送信装置 2 は、AV ストリームを一定単位で暗号化するサイズを通知するための AV ストリーム暗号フレームサイズ通知を受信装置 3 に送信する（ステップ S 4 4

）。もちろん、AVストリーム暗号化通知とAVストリーム暗号フレームサイズ通知は同一のパケットで送ってもよいし、別々なパケットとして順番を入れ替えて送ってもよい。

【0100】

なお、図17では、第2の実施形態の処理手順の一部に、AVストリーム暗号フレームサイズ通知を含める例を説明したが、この通知は第2の実施形態に限ったものではなく、送信装置2が受信装置3に対してAVデータを送信する前であれば、第1の実施形態や第3の実施形態においても適用可能である。

【0101】

(3)は、受信装置3から送信装置2へ処理可能な暗号フレームサイズを通知する方法である。

【0102】

この方法における受信装置3のブロック構成は図18のようになる。図18では、第1～第3の実施形態における受信装置3の内部構成を示した図3と共通する構成部分には同一符号を付しており、以下では相違点を中心に説明する。

【0103】

図3との違いは、著作権保護認証・鍵交換部27の中に暗号フレームサイズ通知送信部30を備えている点と、著作権保護認証・鍵交換部27にて生成された情報がパケット処理部23によってトランスポート層のパケットにカプセル化される点である。

【0104】

暗号フレームサイズ通知送信部30は、著作権保護復号化部24がAVデータを復号する際に処理可能な暗号フレームサイズに関する情報を有しており、このサイズを著作権保護認証・鍵交換処理部27のコマンドの一部として定義しておく。

【0105】

なお、図3では、著作権保護認証・鍵交換部27にて生成された情報は、インターフェース部21によって無線レイヤのフレームにカプセル化されて送信されたが、図18ではパケット処理部23によってTCP/IPパケット化して送信する。

もちろん、図 3 に示した方法と同様に、無線レイヤのフレームにカプセル化して送信するようにしてもよいし、通信処理部 22 を利用して直接データリンク層のフレームにカプセル化して送信するようにしてもよい。

【0106】

また、図 18 では著作権保護復号化部 24 が処理可能な暗号フレームサイズに関する情報を、暗号フレームサイズ通知送信部 30 が有している場合について示したが、(a)著作権保護復号化部 24 が可変の暗号フレームサイズを処理可能な場合、(b)著作権保護復号化部 24 に処理可能な暗号フレームサイズに関する情報が保存されている場合については、暗号フレームサイズ通知送信部 30 が著作権保護復号化部 24 に問い合わせるようにしてもよい。その場合の内部構成は図 19 のようになる。

【0107】

図 20 は(3)の方法における送信装置 2 の構成を示すブロック図である。図 20 では、第 1 から第 3 の実施形態における送信装置 2 の内部構成を示した図 2 と共通する構成部分には同一符号を付しており、以下では相違点を中心に説明する。図 2 との違いは、著作権保護認証・鍵交換部 17 の中に暗号フレームサイズ通知受信部 19 を備えている点と、著作権保護認証・鍵交換部 17 にて生成された情報がパケット処理部 15 によってトランスポート層のパケットにカプセル化される点である。暗号フレームサイズ通知受信部 19 は、著作権保護認証・鍵交換処理部のコマンドの一部として定義された、暗号フレームサイズを通知するコマンドを受信すると、暗号フレームサイズに関する情報を抽出する機能を持つ。さらに、抽出した暗号フレームサイズを著作権保護暗号化部 14 に通知する機能を持つ。

【0108】

著作権保護暗号化部 14 は、受信装置 3 から指定された暗号フレームサイズに従って、AVデータを暗号化する。

【0109】

図 21 は当該方法における暗号フレームサイズの指定方法の処理手順を示すシーケンス図である。認証・鍵交換手順までの手順は第 2 の実施形態と同様の方法

でよい。認証・鍵交換が成立し、送信装置2と受信装置3とでコンテンツの復号化に用いる鍵が共有すると、受信装置3は送信装置2に対して、AVストリーム暗号フレームサイズ通知を行う。受信装置2は、通知されたサイズに従って、AVデータを暗号化し受信装置に対して送信する。

【0110】

なお、送信装置2の著作権保護暗号化部14が処理できないサイズを受信装置3から通知された場合には、逆に送信装置2が受信装置3に対して、暗号化サイズを指定するようなメッセージを送信する機能を持っていてもよい。その場合の送信装置2および受信装置3の内部構成をそれぞれ図22と図23に示される。

【0111】

送信装置2が通知されたサイズの値で処理できない場合とは、たとえば送信装置に指定されたサイズでAVデータを暗号化する機能がない場合や、すでに送信装置がマルチキャストにてAVデータの送信を行っており、途中で暗号フレームサイズを変更することができない場合などを指す。

【0112】

マルチキャスト通信の場合、1台目で送信装置と受信装置の暗号フレームサイズが決定されると、マルチキャスト通信の途中で2台目以降が参加して暗号フレームサイズの指定要求を行ったとしても通信途中でサイズを変更することができない。この場合、送信装置が暗号フレームサイズ(マルチキャスト通信の場合、現在利用している暗号フレームサイズの値)を受信装置に指定することになる。

【0113】

なお、マルチキャスト通信の場合には、上述した方法以外にも、送信装置2と受信装置3があらかじめ合意したマルチキャスト用の暗号フレームサイズとする方法、またはネゴシエーションによって送信装置2と受信装置3があらかじめ合意したマルチキャスト用のサイズとする方法といった、(1)もしくは(1)と(2)、(3)を組み合わせた方法をとることができる。

【0114】

図24はマルチキャスト通信において、送信装置2と受信装置3があらかじめ合意したマルチキャスト用の暗号フレームサイズにてAVデータを暗号化する処理

手順を示すシーケンス図である。送信装置 2 が AV データをマルチキャストにて送信する場合、あらかじめ定められたマルチキャスト用の暗号フレームサイズに従って AV データを暗号化して送信する。受信装置 3 は、マルチキャストにて受信した AV データをあらかじめ定められたマルチキャスト用の暗号フレームサイズに従って復号する。

【0115】

このように、マルチキャスト通信以外の場合とマルチキャスト通信の場合とで、暗号フレームサイズを分ける。これにより、送信装置 2 が AV データを送信途中で追加的に参加してきた受信装置に対して、通信途中で暗号フレームサイズを変更する必要がなく、また AV データが受信できないような受信装置 3 の開発を未然に防ぐことができる。もちろん、マルチキャスト専用の暗号フレームサイズをあらかじめ複数定義しておき、その中から (2) または (3) で示したネゴシエーションの方法により送信装置 2 と受信装置 3 が選択するような方法になっていてもよい。

【0116】

このマルチキャスト専用の暗号フレームサイズを定義する方法における受信装置 3 のブロック構成は図 25 のようになる。図 18 との違いは、マルチキャスト用暗号フレームサイズ通知部 31 を備えている点である。マルチキャストにて AV データを受信した場合には、マルチキャスト用暗号フレームサイズ通知部 31 は、マルチキャスト用の暗号フレームサイズを著作権保護復号化部 24 に通知する機能を持つ。

【0117】

著作権保護復号化部 24 は、受信装置 3 から受信した AV データをマルチキャスト用暗号フレームサイズ通知部 31 によって通知された暗号フレームサイズに従って復号化する。

【0118】

また送信装置 2 のブロック構成は図 26 のようになる。図 20 との違いは、マルチキャスト用暗号フレームサイズ通知部 20 を備えている点である。マルチキャストにて AV データを送信する場合には、マルチキャスト用暗号フレームサイズ

通知部 20 は、マルチキャスト用の暗号フレームサイズを著作権保護暗号化部 14 に通知する機能を持つ。著作権保護暗号化部 14 は、AV データを通知された暗号フレームサイズに従って暗号化する。

【0119】

図 27 はこれら暗号フレームサイズのネゴシエーションに使うデータフォーマットの一例を示す図である。サイズ指定要求パケットは、受信装置 3 が送信装置 2 に処理可能な暗号フレームサイズの指定を行う際に用いられ、IP ヘッダ d 21 と、TCP ヘッダ d 22 と、著作権保護用共通制御ヘッダ d 23 と、暗号フレームサイズ要求 d 24 と、サイズの値 d 25 とを有する。

【0120】

サイズ指定応答パケットは、サイズ指定要求パケットを受信した送信装置 2 が指定されたサイズでの送信を許可するか、拒絶する際に用いられ、IP ヘッダ d 31 と、TCP ヘッダ d 32 と、著作権保護用共通制御ヘッダ d 33 と、暗号フレームサイズ応答 d 34 と、サイズの値 d 35 とを有する。

【0121】

サイズ指定応答パケットのサイズの値は、拒絶する際には必須となるが、許可する際には値を入れても入れなくても、どちらでもよい。

【0122】

また、ここでは、第 2 の実施形態の処理手順の一部として AV ストリーム暗号フレームサイズ通知を含めたが、この通知は第 2 の実施形態に限ったものではなく、受信装置 3 が送信装置 2 から復号化可能な状態で AV データを受信する前であれば第 1 の実施形態や第 3 の実施形態においても適用可能である。ここで復号可能な状態とは、送信装置 2 と受信装置 3 の間で認証・鍵交換が成立し、受信した AV ストリームを復号化できる状態にあることを指す。

【0123】

このように、第 4 の実施形態によれば、受信装置 3 から送信装置 2 に処理可能な暗号フレームサイズを通知するため、受信装置 3 は用途に合わせた暗号フレームサイズを処理可能な暗号処理モジュールを実装することができ、機器の製造コストをおさえることができる。

【0124】

例えば、携帯型オーディオ機器の場合には、AVデータのデータサイズも小さく、また送信レートも低い。このためセキュリティ上の観点から暗号フレームサイズを小さくすることが望ましい。一方、有線接続される高解像度の画像が受信可能なテレビなどは、AVデータのサイズも大きく送信レートも高い。このため、暗号フレームサイズを大きくすることが望ましい。なぜならば暗号フレームサイズが小さい場合、大量のデータを小さなサイズに区切って暗号・復号処理を施さなければならず、そのための高速の処理モジュールを備える必要があるため、機器のコストが増大するためである。また、下位のネットワークレイヤによっても適切な暗号フレームサイズは異なる。例えば、トランスポート層のプロトコルとしてUDPを用いるとする。データリンク層の最大パケットサイズを越えたUDPパケットを送信しようとする、1つのUDPパケットは複数のデータリンクフレームに分割される。UDPは再送処理機構を備えていないため、この時分割されたデータリンクフレームのうち、1つのフレームでも欠落した場合には、UDPパケット全体が損失することになる。この時の暗号フレームサイズを大きく決定した場合、1つのUDPフレームが欠落した場合、その暗号フレームサイズのデータを復号化することができなくなってしまう。このように転送効率を考慮して、暗号フレームサイズをデータリンクフレームのサイズにあわせて送信することがある。

【0125】

このように機器の性能やAVデータの特性、ネットワークの特性によって適切な暗号フレームサイズは異なるため、ネゴシエーション処理を行い、その都度適切な暗号化サイズを決定することが望ましい。

【0126】

上述した図6～図8の処理は、ハードウェアで実現してもよいし、ソフトウェアで実現してもよい。ソフトウェアで実現する場合には、図6～図8の処理の少なくとも一部を実現するプログラムをフロッピーディスクやCD-ROM等の記録媒体に収納し、コンピュータに読み込ませて実行させてもよい。記録媒体は、磁気ディスクや光ディスク等の携帯可能なものに限定されず、ハードディスク装置やメモリなどの固定型の記録媒体でもよい。

【0127】

また、図6～図8の処理の少なくとも一部の機能を実現するプログラムを、インターネット等の通信回線（無線通信も含む）を介して頒布してもよい。さらに、同プログラムを暗号化したり、変調をかけたり、圧縮した状態で、インターネット等の有線回線や無線回線を介して、あるいは記録媒体に収納して頒布してもよい。

【0128】

上述した実施形態で説明した送信装置2及び受信装置3は、ハードウェアで構成してもよいし、ソフトウェアで構成してもよい。ソフトウェアで構成する場合には、送信装置2及び受信装置3の少なくとも一部の機能を実現するプログラムをフロッピーディスクやCD-ROM等の記録媒体に収納し、コンピュータに読み込ませて実行させてもよい。記録媒体は、磁気ディスクや光ディスク等の携帯可能なものに限定されず、ハードディスク装置やメモリなどの固定型の記録媒体でもよい。

【0129】

また、送信装置2及び受信装置3の少なくとも一部の機能を実現するプログラムを、インターネット等の通信回線（無線通信も含む）を介して頒布してもよい。さらに、同プログラムを暗号化したり、変調をかけたり、圧縮した状態で、インターネット等の有線回線や無線回線を介して、あるいは記録媒体に収納して頒布してもよい。

【0130】

【発明の効果】

以上詳細に説明したように、本発明によれば、ネゴシエーションしたペイロードタイプの値を含むパケットを送信装置と受信装置との間で送受するため、そのパケットに含まれる電子データが著作権保護を図る必要があるか否かを識別でき、著作権保護を図りつつ、電子データを簡易かつ迅速に送受信できる。

【図面の簡単な説明】

【図1】

本発明の一実施形態である送信装置と受信装置とを備えたAV通信システムの概

略構成を示すブロック図。

【図 2】

送信装置の内部構成の一例を示すブロック図。

【図 3】

受信装置の内部構成の一例を示すブロック図。

【図 4】

送信装置と受信装置でやり取りされるデータフォーマットを示す図。

【図 5】

図 4 のより詳細なデータフォーマットを示す図。

【図 6】

送信装置と受信装置が行う AV データの暗号化伝送処理の第 1 の実施形態の処理手順を示すシーケンス図。

【図 7】

著作権保護用制御データ d 8 のデータフォーマットを示す図。

【図 8】

従来の K a , K b , K z の処理方法を示す図。

【図 9】

送信装置のコンテンツ鍵更新の検出処理手順を示すシーケンス図。

【図 1 0】

シード値を下位 1 ビットにした場合の処理手順の一例を示すフローチャート。

【図 1 1】

パケットロスが発生した場合の処理手順の一例を示すフローチャート。

【図 1 2】

シード値が複数ビットの場合の処理手順の一例を示すフローチャート。

【図 1 3】

著作権保護用制御データ d 8 の中に含めるシード値 K b を、下位複数ビットに設定する場合の受信装置 3 の内部構成を示すブロック図。

【図 1 4】

送信装置 2 と受信装置 3 が行う AV データの暗号化伝送処理の第 2 の実施形態の

処理手順を示すシーケンス図。

【図 15】

受信装置 3 が送信装置 2 に対して所望の AV データを指定し、その指定に対する応答として、当該 AV データが暗号化されていることを通知する場合の処理手順を示すシーケンス図。

【図 16】

送信装置 2 と受信装置 3 が行う AV データの暗号化伝送処理の第 3 の実施形態の処理手順を示すシーケンス図。

【図 17】

送信装置 2 と受信装置 3 が行う AV データの暗号化伝送処理の第 3 の実施形態の処理手順を示すシーケンス図。

【図 18】

暗号フレームサイズ通知送信部を有する受信装置の内部構成を示すブロック図。

【図 19】

図 18 の変形例を示すブロック図。

【図 20】

暗号フレームサイズ通知受信部を有する送信装置の内部構成を示すブロック図。

【図 21】

暗号フレームサイズの指定方法の処理手順を示すシーケンス図。

【図 22】

暗号フレームサイズの指定を行う受信装置の内部構成を示すブロック図。

【図 23】

暗号フレームサイズの指定を受ける送信装置の内部構成を示すブロック図。

【図 24】

マルチキャスト通信において、送信装置と受信装置があらかじめ合意したマルチキャスト用の暗号フレームサイズにて AV データを暗号化する処理手順を示すシーケンス図。

【図 25】

マルチキャスト専用の暗号フレームサイズを定義する場合の受信装置のブロック図。

【図 26】

マルチキャスト専用の暗号フレームサイズを定義する場合の送信装置のブロック図。

【図 27】

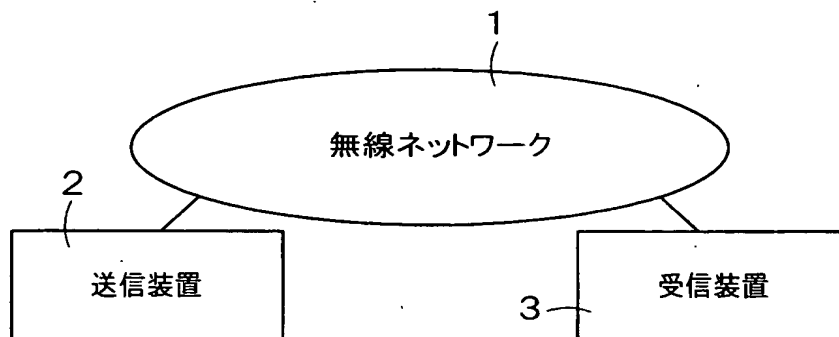
サイズ指定要求パケットとサイズ指定応答パケットのデータフォーマットを示す図。

【符号の説明】

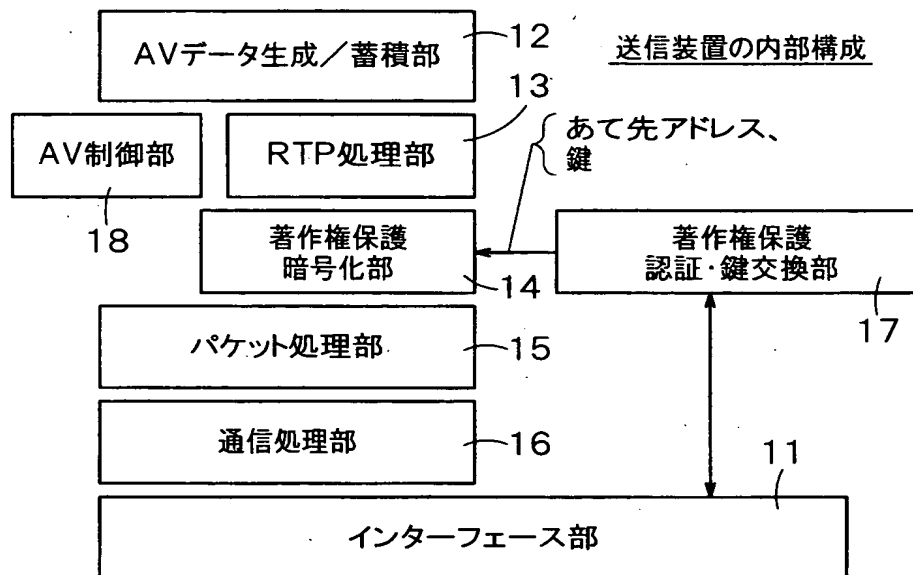
- 1 ホームネットワーク
- 2 送信装置
- 3 受信装置
- 11 インタフェース部
- 12 AVデータ生成／蓄積部
- 13 RTP処理部
- 14 著作権保護暗号化部
- 15 TCP/IPパケット送受信部
- 16 イーサネットフレーム送受信部
- 17 著作権保護認証・鍵交換部
- 21 インタフェース部
- 22 イーサネットフレーム送受信部
- 23 TCP/IPパケット送受信部
- 24 著作権保護復号化部
- 25 RTP処理部
- 26 AVデータ再生／蓄積部
- 27 著作権保護認証・鍵交換部

【書類名】 図面

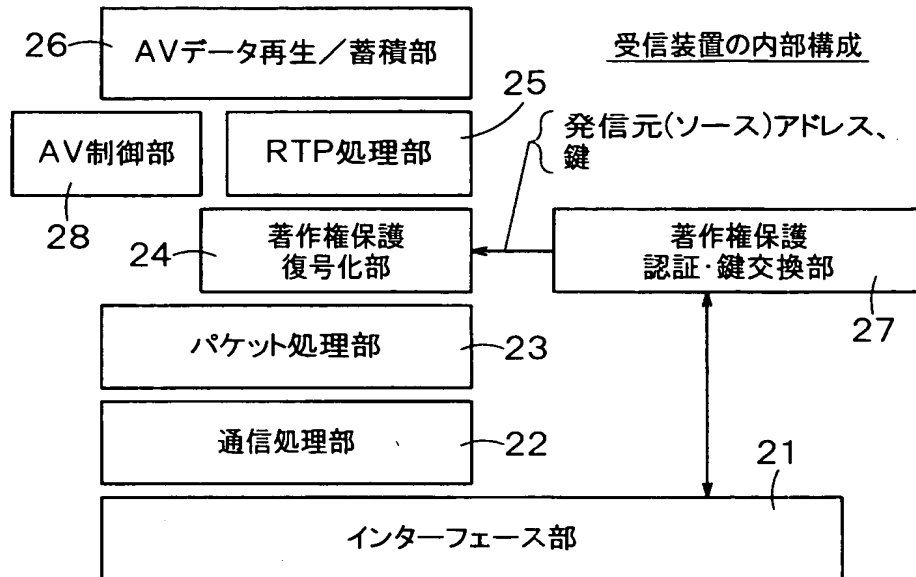
【図 1】



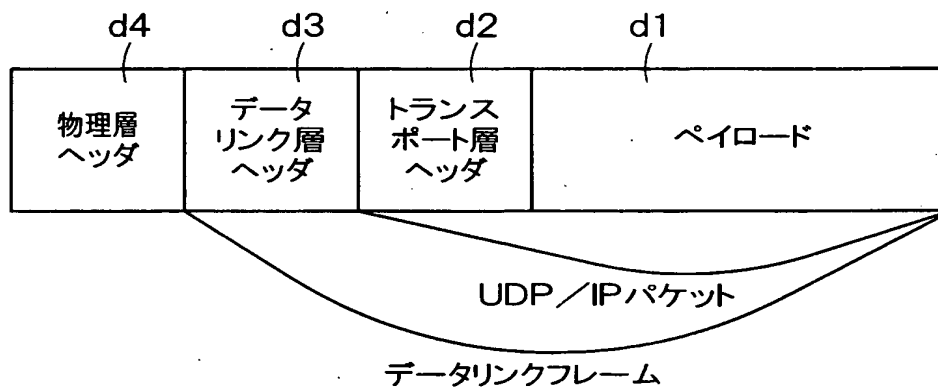
【図 2】



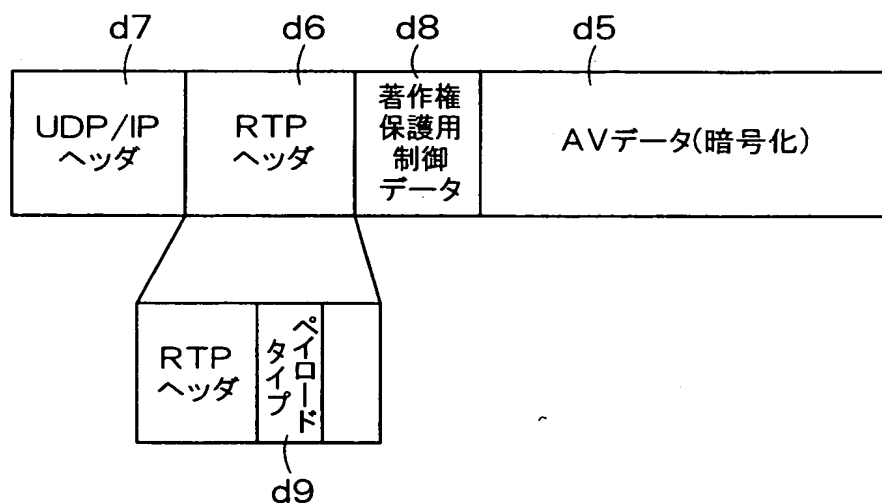
【図3】



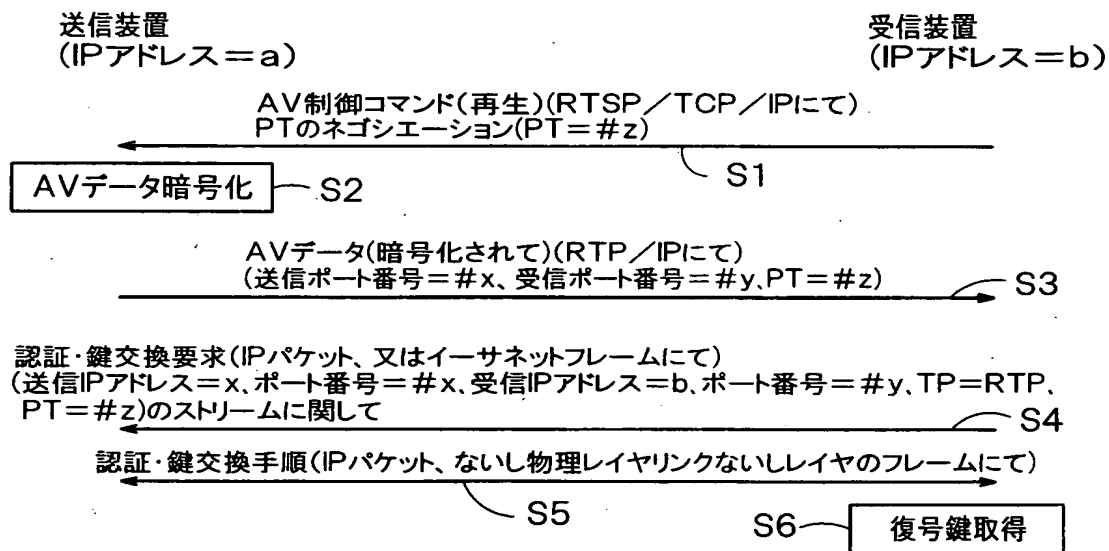
【図4】



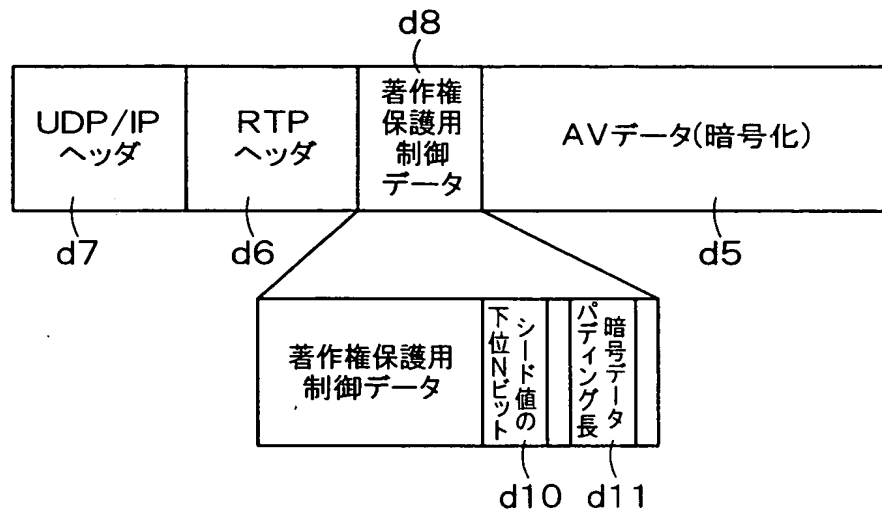
【図 5】



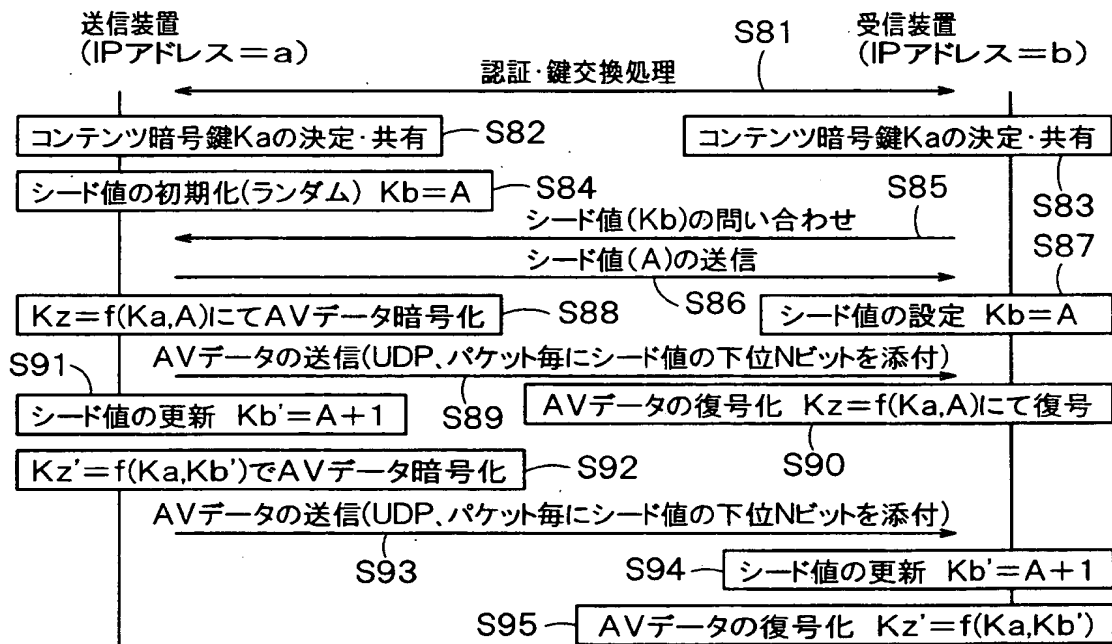
【図 6】



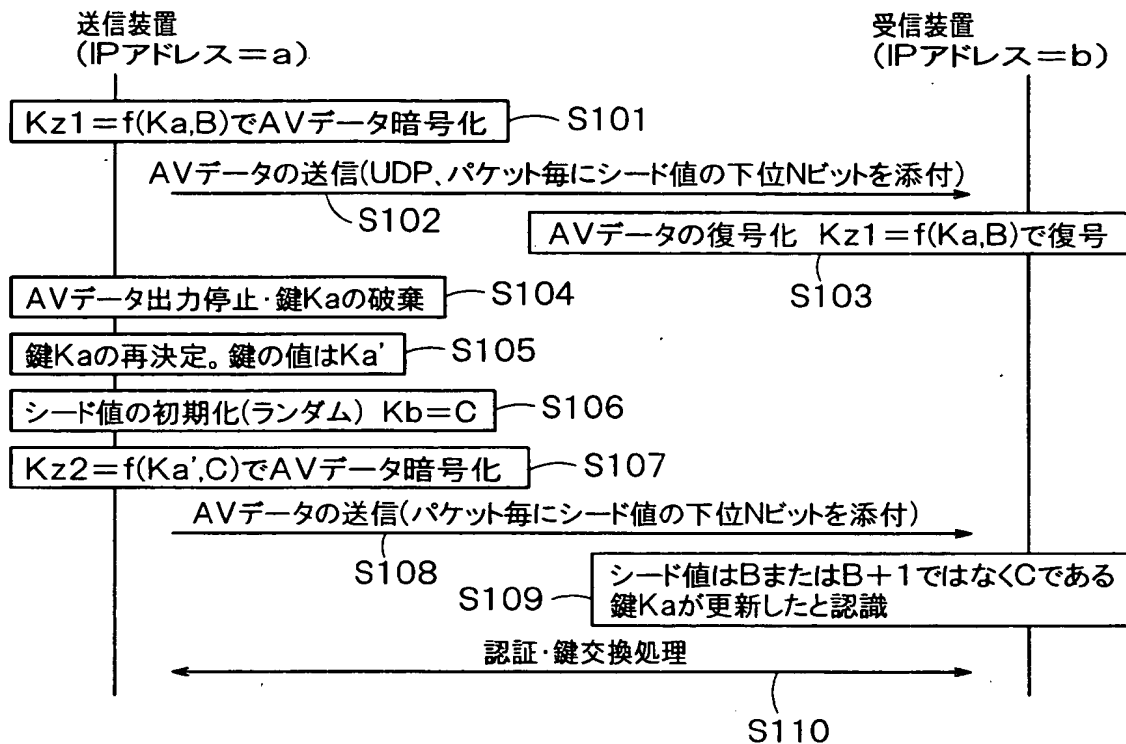
【図 7】



【図 8】

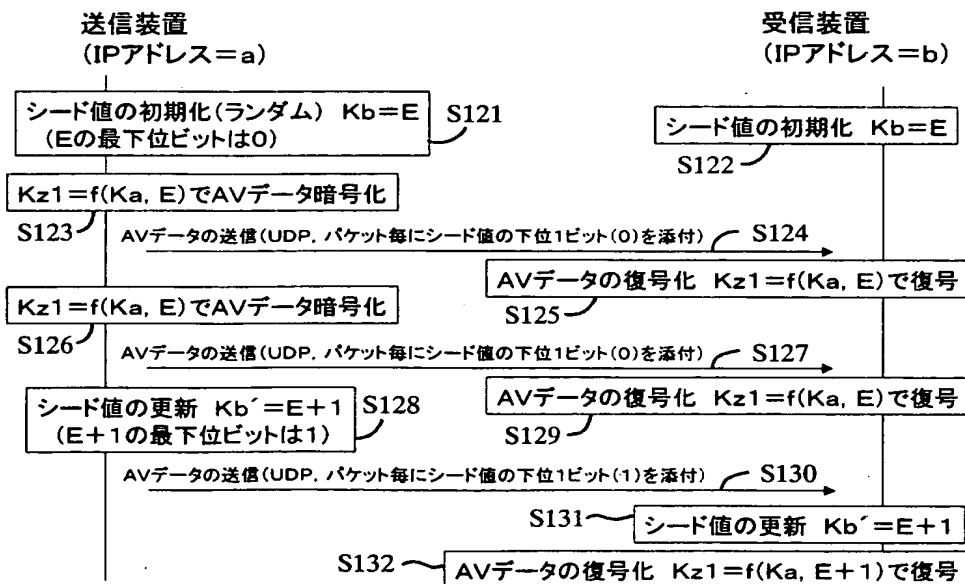


【図 9】



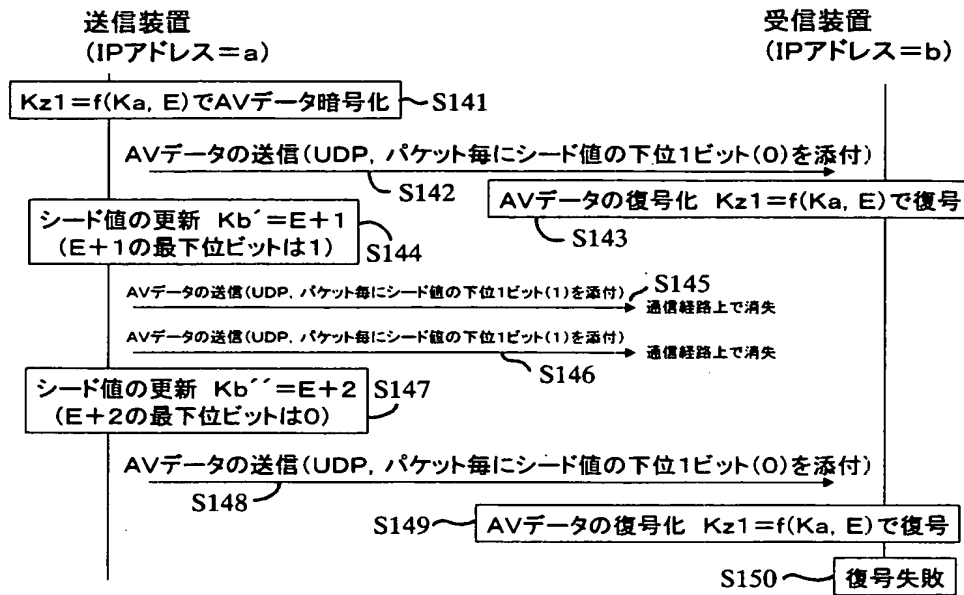
【図 10】

シード値1ビットの場合の処理手順



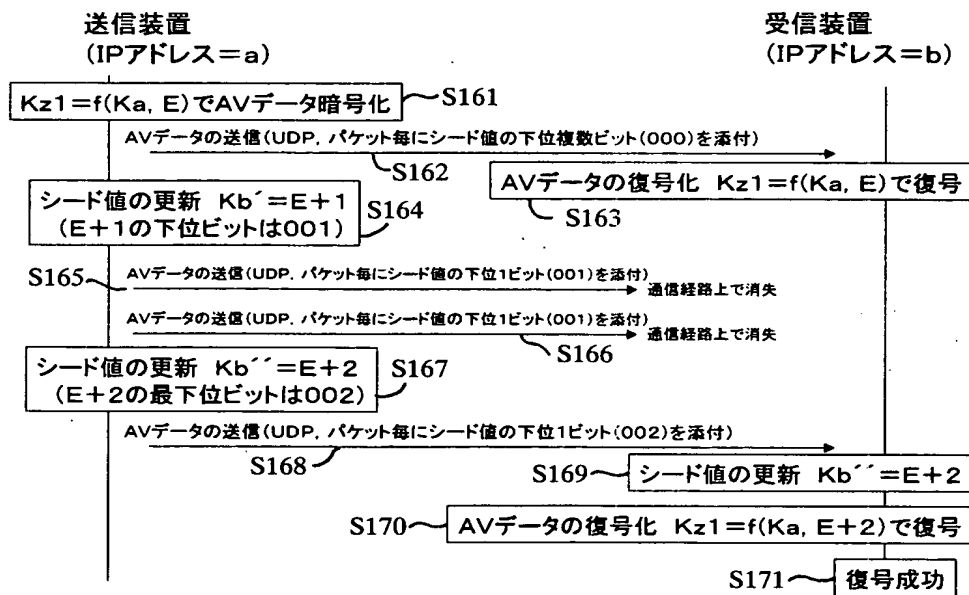
【図 1 1】

シード値1ビットの場合の処理手順(パケットロス発生時)

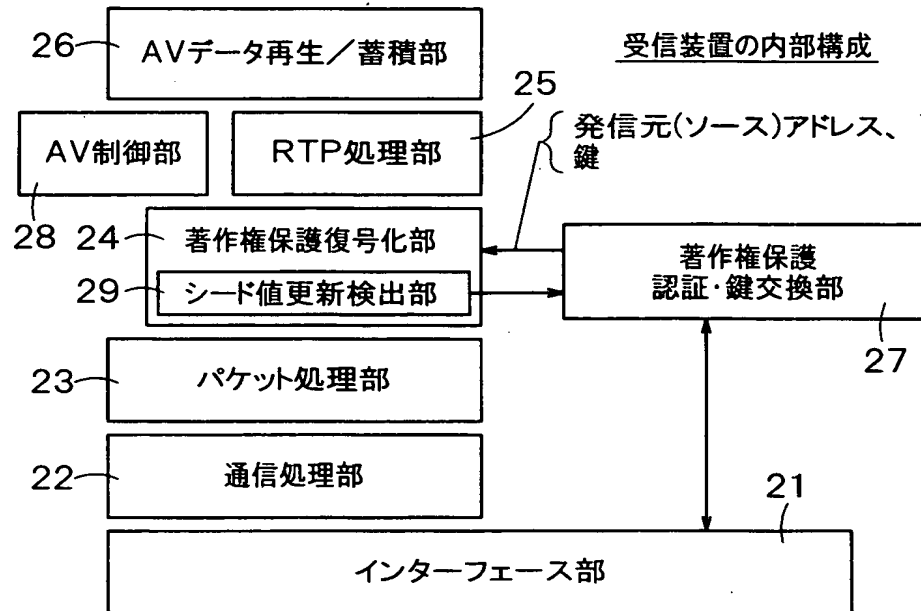


【図 1 2】

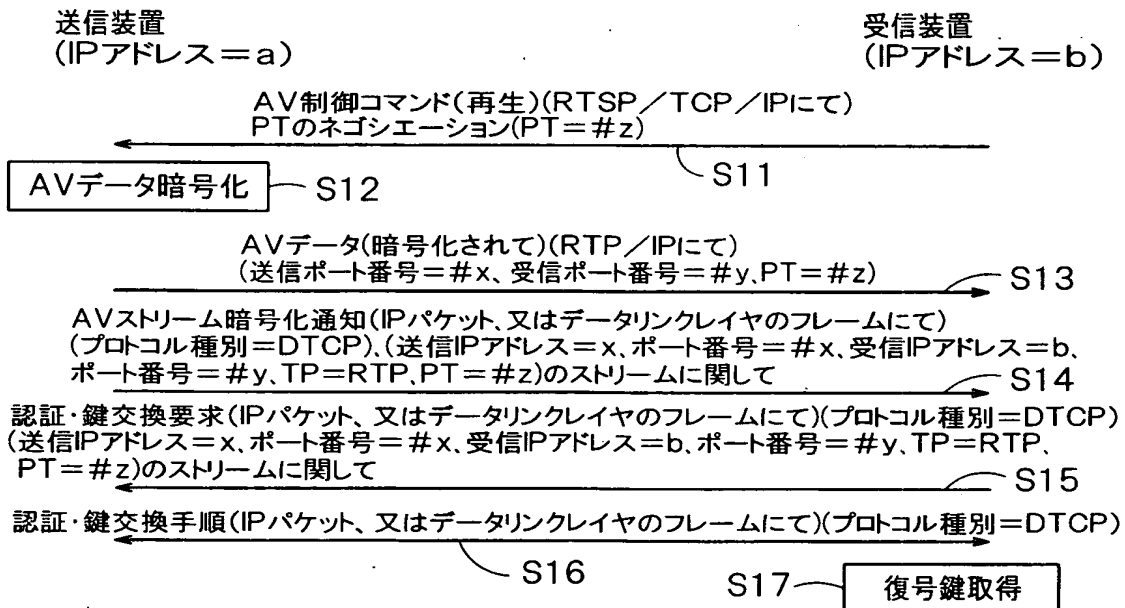
シード値複数ビットの場合の処理手順



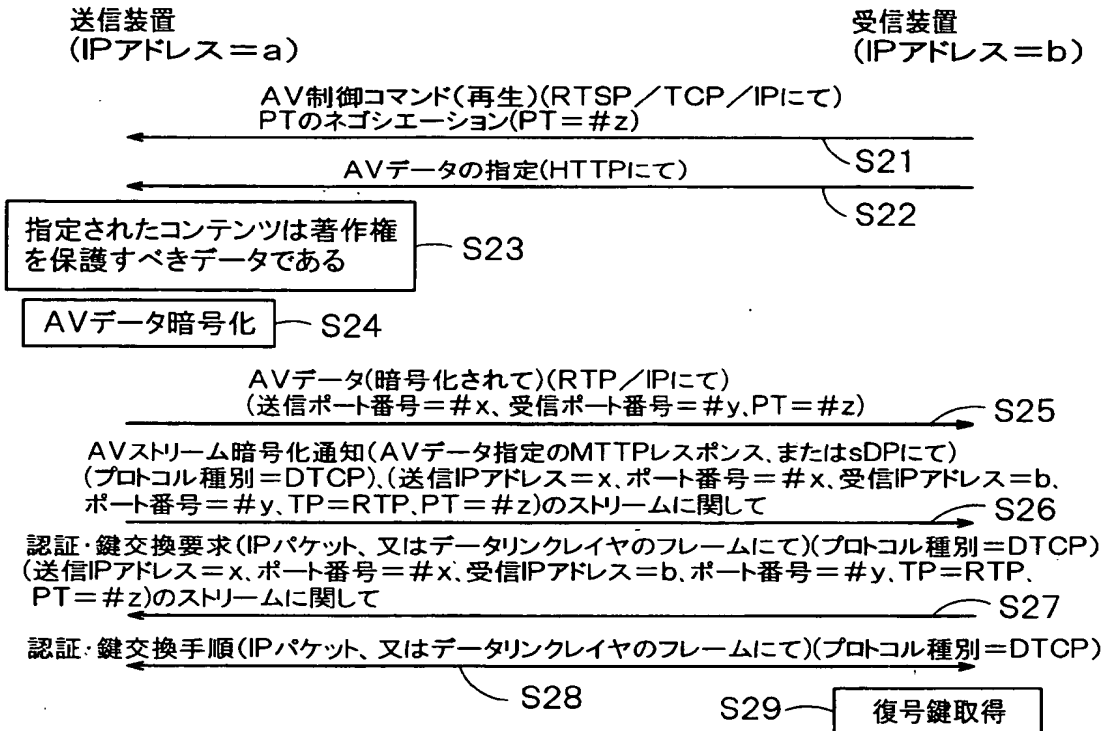
【図 13】



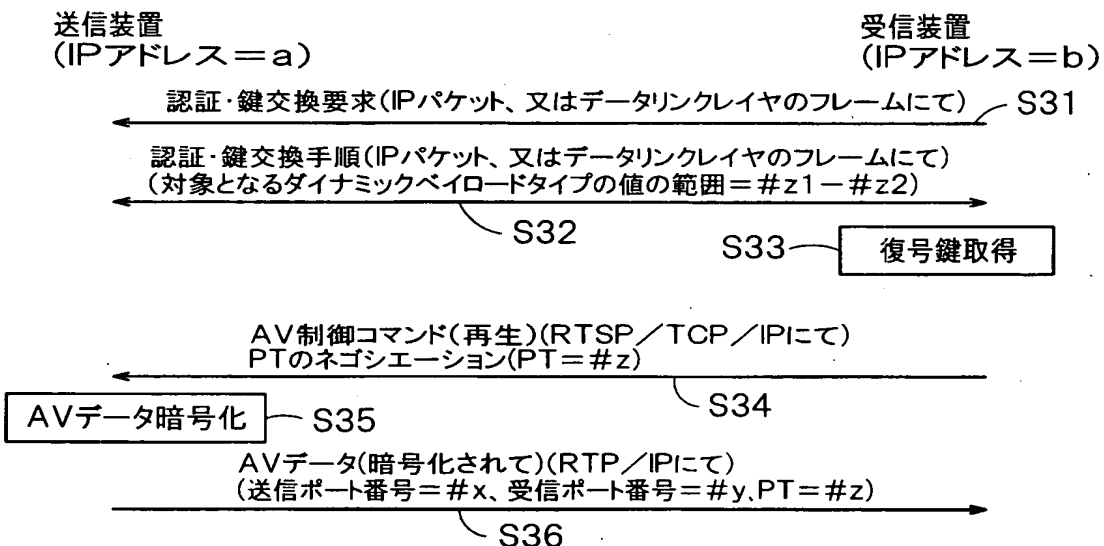
【図 14】



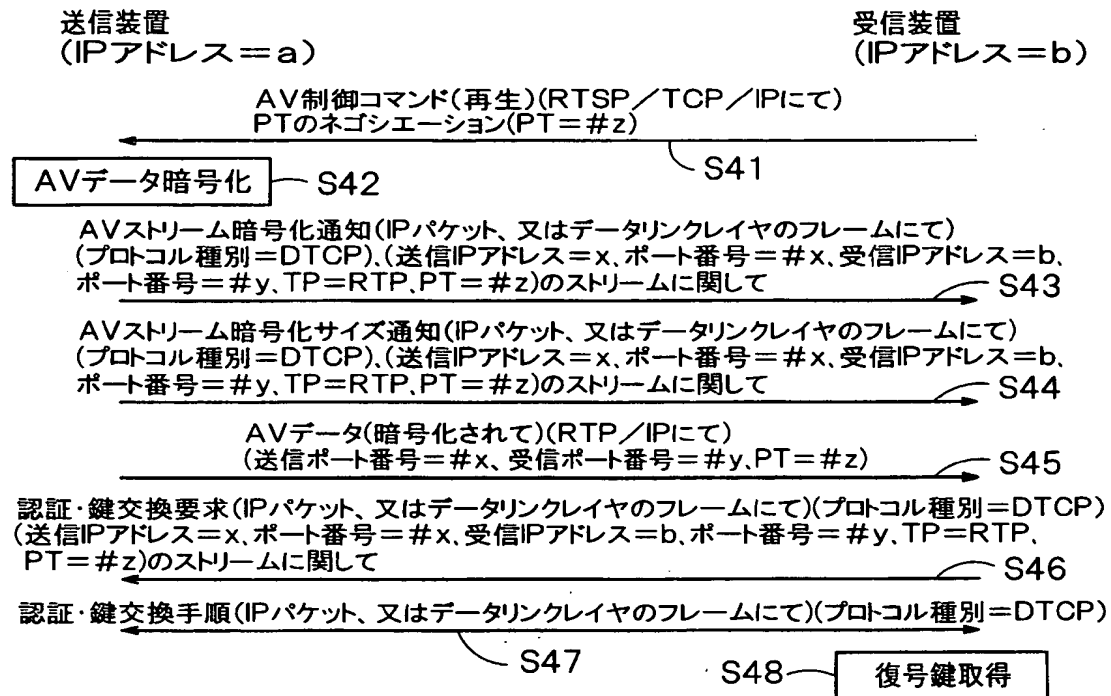
【図 15】



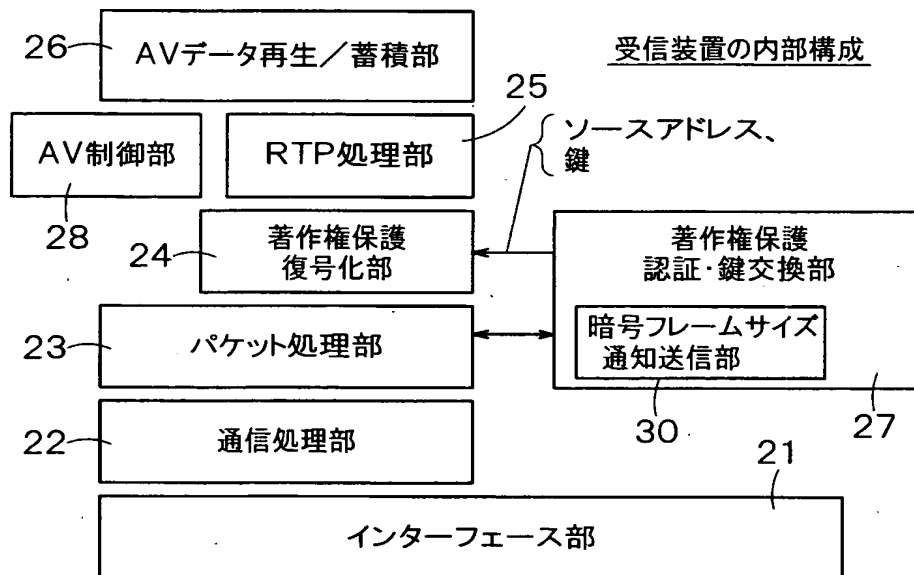
【図 16】

注: ($\#z1 \leq \#z \leq \#z2$)

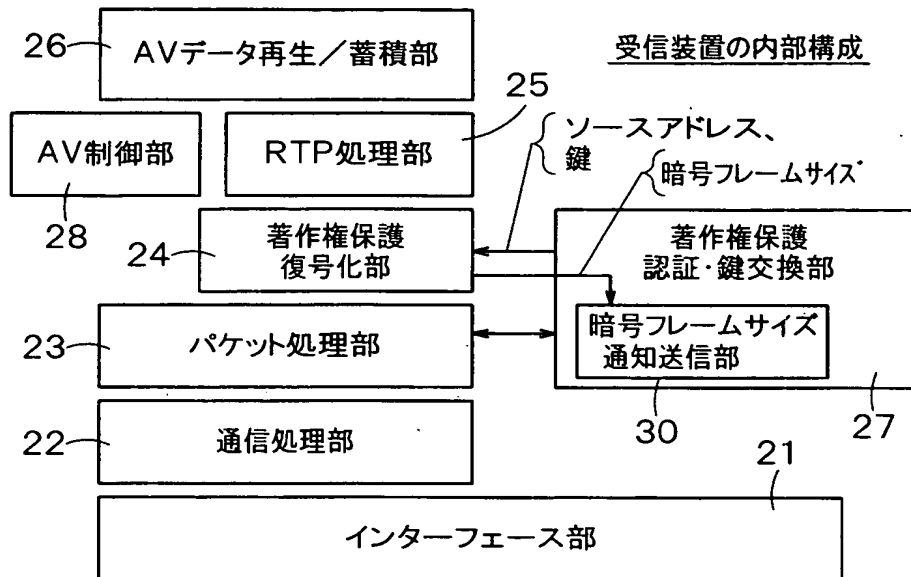
【図 17】



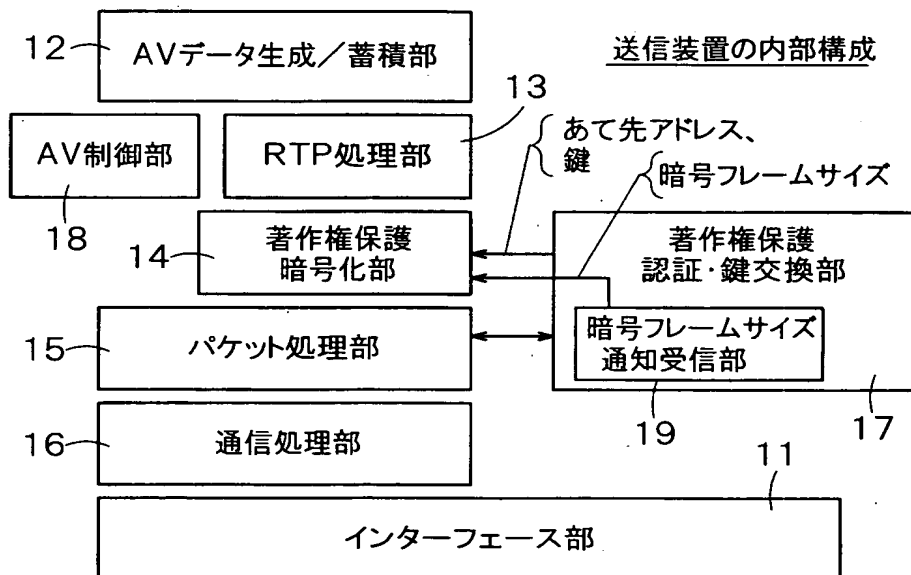
【図 18】



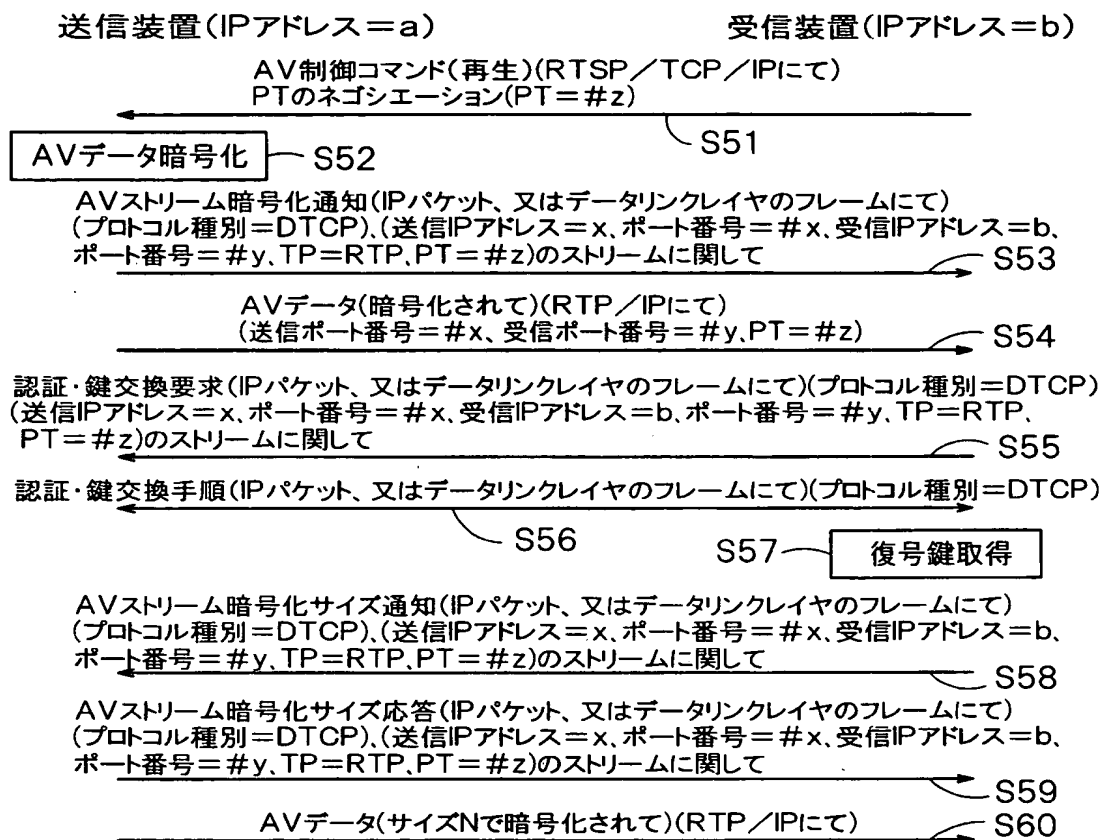
【図 19】



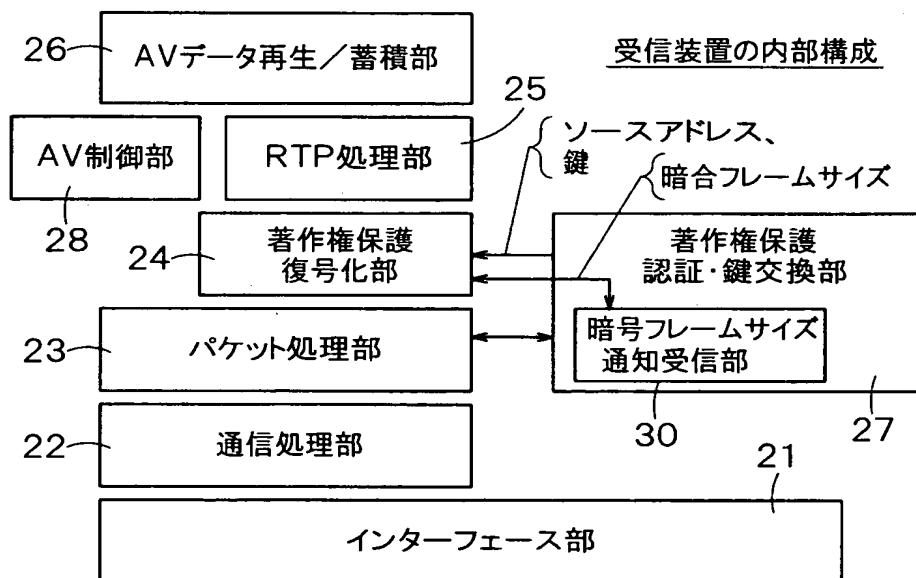
【図 20】



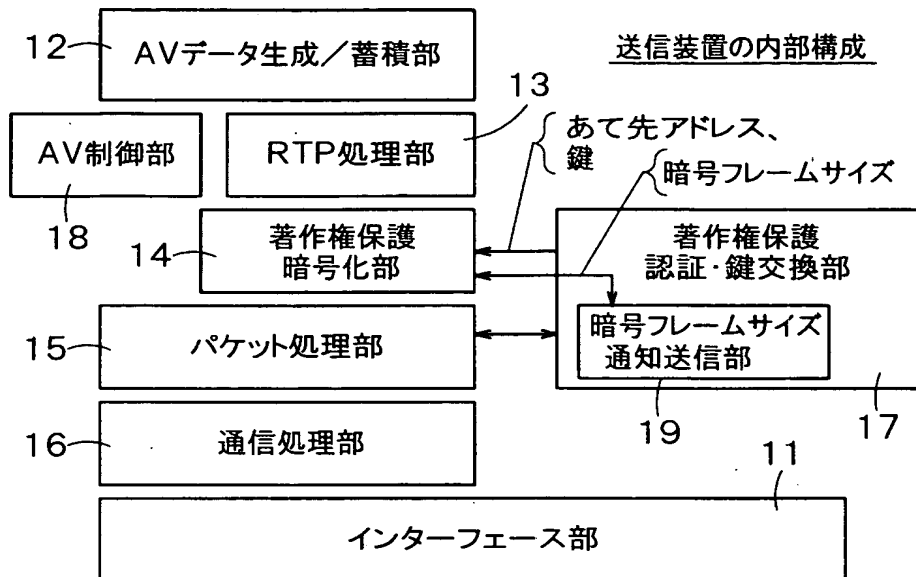
【図 2 1】



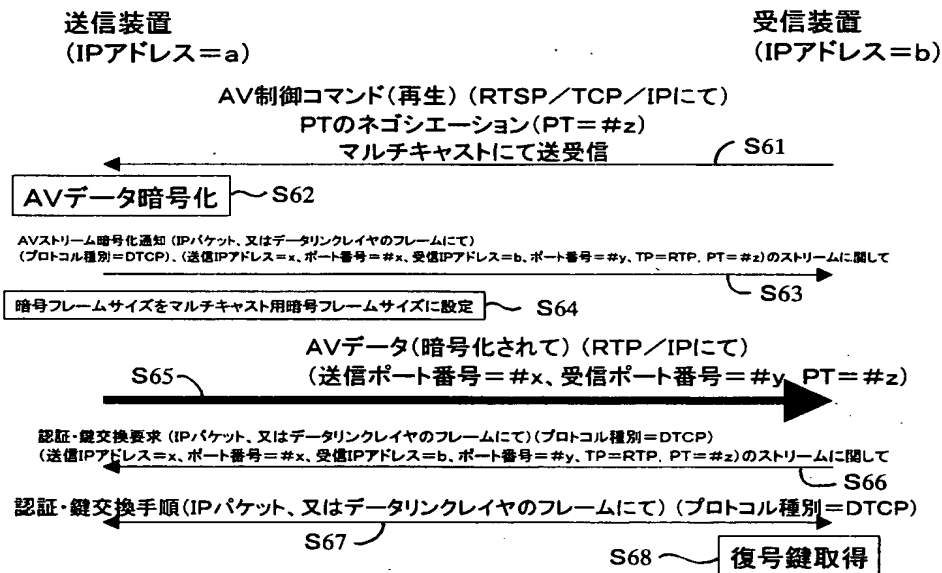
【図 2 2】



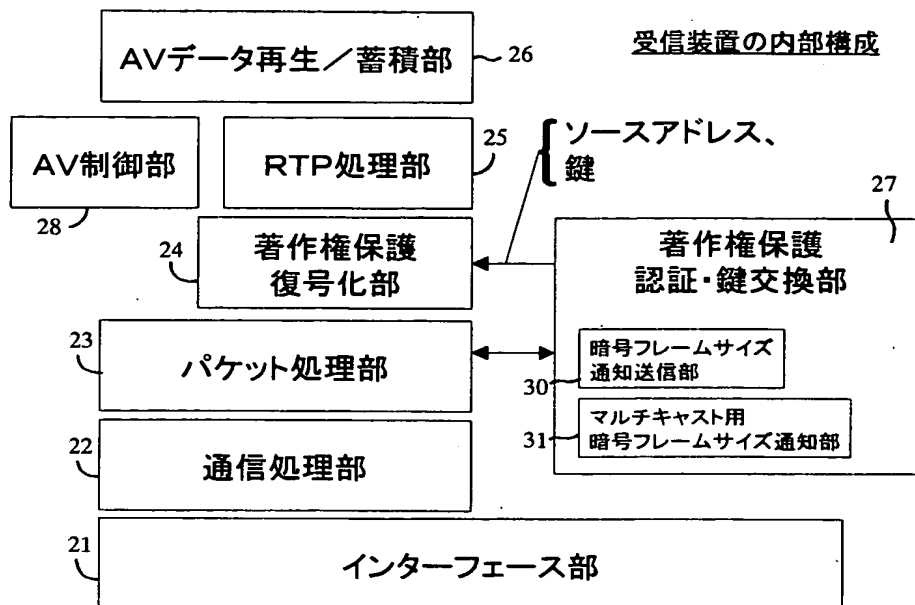
【図 23】



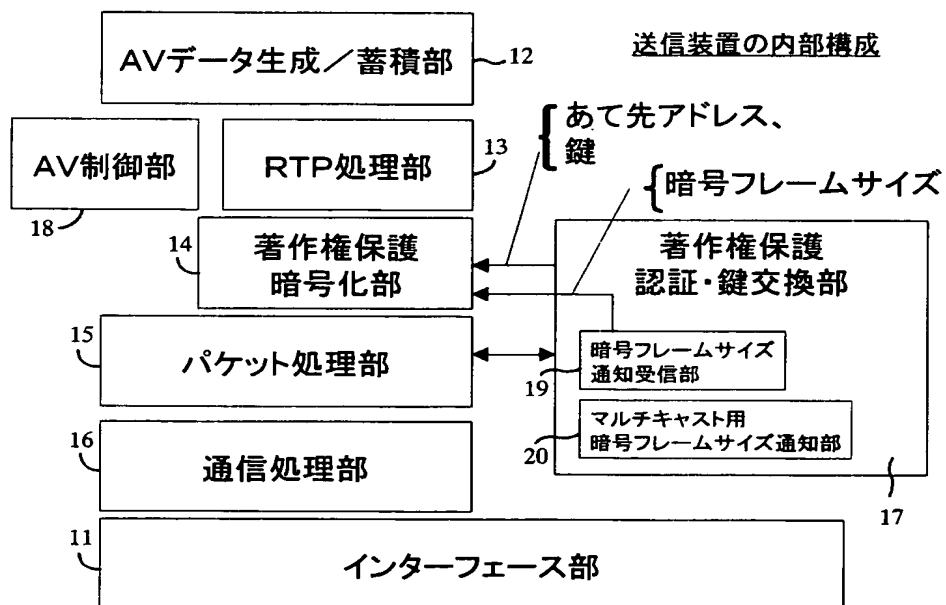
【図 24】



【図 25】

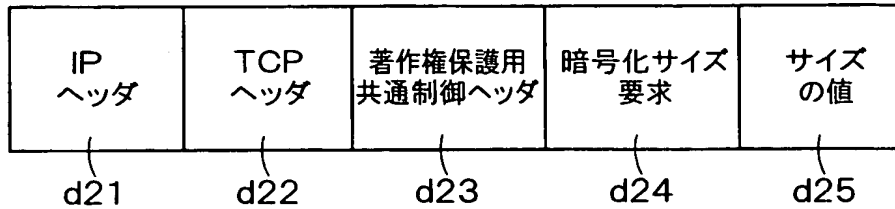


【図 26】

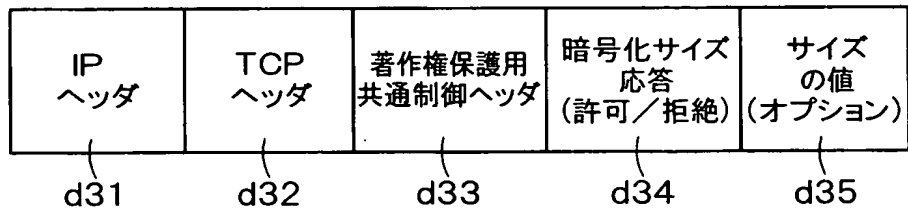


【図 27】

サイズ指定要求パケット



サイズ指定応答パケット



【書類名】 要約書

【要約】

【課題】 著作権保護を図りつつ電子データの送信または受信を行えるようにする。

【解決手段】 AV通信システムは、ある家庭内のホームネットワーク 1 と、このホームネットワーク 1 に接続されている送信装置 2 及び受信装置 3 とを備えている。著作権保護の必要なAVデータを暗号化したペイロードに、プロトコル種別（例えばRTP）と、このプロトコルが使用するペイロードタイプの値と、を付加したAVストリームを送信装置 2 から受信装置 3 に送信するため、このAVストリームを受信した受信装置 3 は、AVデータが暗号化されていることを容易に検出でき、かつ認証・鍵交換が必要なデータを容易に識別できる。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2003-173985
受付番号	50301019999
書類名	特許願
担当官	第一担当上席 0090
作成日	平成 15 年 6 月 23 日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000003078
【住所又は居所】	東京都港区芝浦一丁目 1 番 1 号
【氏名又は名称】	株式会社東芝

【代理人】

申請人

【識別番号】	100075812
【住所又は居所】	東京都千代田区丸の内 3-2-3 協和特許法律事務所
【氏名又は名称】	吉武 賢次

【選任した代理人】

【識別番号】	100088889
【住所又は居所】	東京都千代田区丸の内 3 丁目 2 番 3 号 協和特許法律事務所
【氏名又は名称】	橋谷 英俊

【選任した代理人】

【識別番号】	100082991
【住所又は居所】	東京都千代田区丸の内 3 丁目 2 番 3 号 富士ビル 協和特許法律事務所
【氏名又は名称】	佐藤 泰和

【選任した代理人】

【識別番号】	100096921
【住所又は居所】	東京都千代田区丸の内 3-2-3 富士ビル 3 階 協和特許法律事務所
【氏名又は名称】	吉元 弘

【選任した代理人】

【識別番号】	100103263
【住所又は居所】	東京都千代田区丸の内 3 丁目 2 番 3 号 協和特許法律事務所

次頁有

認定・付加情報 (続き)

【氏名又は名称】 川崎 康

次頁無

特願 2003-173985

出願人履歴情報

識別番号

[000003078]

1. 変更年月日 2001年 7月 2日
[変更理由] 住所変更
 住 所 東京都港区芝浦一丁目1番1号
 氏 名 株式会社東芝

2. 変更年月日 2003年 5月 9日
[変更理由] 名称変更
 住所変更
 住 所 東京都港区芝浦一丁目1番1号
 氏 名 株式会社東芝